Data Mining and Risk Assessment Application
v. 3.0
User Manual

DRAFT

Prepared for:
DoD Purchase Card Program Management Office

Abstract This guide describes how to use the PCOLS Data Mining and Risk Assessment Application.

Document Date Feb 2010

Document Version 3.1

Document History

Document Version	Date	Description
1.0	January 2009	DM/RA Merged
2.0	February 2009	Updated
3.0	April 2009	Updated
3.1	February 2010	Updated Help Desk contact info

DRAFT

Table of Contents

1. Introduction **2**
2. DM/RA Users and Hierarchy **5**
3. Logon Functions **6**
4. Navigation **7**
4.1 General Navigation 7
4.2 Data Mining Navigation 7
4.3 Risk Assessment Navigation 9
5. Data Mining Application **10**
5.1 Introduction 10
5.2 DM User Hierarchy 10
5.3 Case Management 11
5.4 Find Transactions 26
6. Risk Assessment Application **28**
6.1 Introduction 28
6.2 RA User Hierarchy 28
6.3 RA Controls 29
6.4 RA Dashboards 30
6.5 Viewing Control Reports 44
6.6 Accessing Control Reports 69
6.7 Viewing Quarterly Reports 77
Appendix A: Abbreviations, Acronyms, and Definitions **80**

DRAFT

1. Introduction

1.1 Purpose

The Data Mining/Risk Assessment (DM/RA) Application is part of a suite of electronic applications known collectively as the Purchase Card On-line System (PCOLS). The PCOLS consists of the following applications:

- Enterprise Monitoring and Management of Accounts (EMMA) Application,
- Authorization, Issuance and Maintenance (AIM) Application,
- Data Mining (DM)/Risk Assessment (RA) Application.

The purpose of the DM/RA Application User Manual is to provide a concise, accessible instruction guide for authorized users to learn the functionality of the DM/RA Application.

1.2 DM Application Overview

The Data Mining component of the DM/RA Application provides a single user interface for all DoD users to access all DoD purchase card transaction data. The Data Mining Application programmatically reviews 100% of the purchase card transactions. Each transaction is assigned a score by the Risk Predictive Model, which is an integral part of the DM Application. High risk transactions are subsequently referred for review. Also, a statistically based sample of random transactions is referred for review. The Case Manager, also a part of the DM Application, interprets the referred transactions and creates specific cases that are assigned to the Approving/Billing Officials (A/BOs) for review. Through the use of the Case Manager Interview Process, the A/BO demonstrates that due diligence is exercised in the review of the referred transactions. Additionally, the interview process records information related to the data provided to support the validity of the purchase card transaction.

The DM Application uses industry leading analytic techniques, DoD specific business rules, transaction scoring, unique adaptive techniques and learning from historical transaction profiles to flag the transactions for review.

This functionality is accomplished through the following two components within the DM Application - Case Management System and Find Transactions:

- **Case Management System -** This component allows for the review and documentation of all transactions identified through one of the following methods.
    1. **Transaction Identification Methods**
        i. **Neural networks -** to detect abnormal behavior and predict high risk transactions.
        ii. **Profiles -** work with the neural network models to encode and make use of the unique behavior of each individual cardholder and managing account.
        iii. **Random Transactions -** select additional transactions from a statistically based random sampling for review by the A/BO.

DRAFT

iv. **Manual Case Creation for Review -** allows the A/BO to self initiate a case for any transaction in the Case Management system.

2. **Independent Review -** After the referred case has been reviewed by the A/BO, the transaction is available for independent review by authorized DoD Personnel.
3. **Escalation of Open Cases -** The notification functionality is governed by the DM/RA hierarchy (described in Section 2) and accountability and timely adherence to reviewing referred cases. Cases are escalated up the hierarchical chain if they are not initiated or reviewed in a timely manner.

- **Find Transactions -** This component provides complete access to all cardholder transaction data for the previous 18 months and interfaces directly with the Case Management system. In addition to the flagged transactions referred by the application, the Find Transactions component allows users to easily search all transactions through detailed filters (described in Section 5.4).

1.3 RA Application Overview

The RA component of the DM/RA Application uses internal controls and measures, coupled with results from the DM Application, to assess and report on the overall "health" of the DoD organization's purchase card program. The RA Application allows users to monitor risks associated with their purchase card program. Users assess the risk of their purchase card program by monitoring certain risk controls on a billing cycle-by-cycle basis.

This monitoring is accomplished through three components within the RA Application:

- **Controls -** Controls are risk indicators for which exceptions that exceed pre-determined thresholds are monitored. A Control Report provides details of all exceptions that are identified for a particular control.
- **Dashboards -** A Dashboard is the primary component that assesses the risk of the purchase card program at the user's hierarchical level. Within the dashboard risk is assessed for each individual control. Additionally, a cumulative risk assessment for the overall hierarchical level is calculated based on each individual control's risk assessment.
- **Quarterly Reports -** Quarterly Reports provide a three-billing cycle, side-by-side snapshot of the controls' exceptions allowing users to analyze the progress in addressing identified risks for the quarter.

1.4 Data Updates

The Defense Manpower Data Center (DMDC) receives daily transaction data from the banks and, if necessary, adds additional data elements required for DM. The DMDC transmits batch transactions data to the DM/RA Application on a nightly basis using a secure file transfer mechanism.

Dashboards and Control Reports are available to users by billing cycle in the RA Application. A cycle for a cardholder account closes on the 19th of each month. For example, the August billing cycle begins on the 20th day of July and runs through August 19th. The DM/RA Reports for the

DRAFT

most recently completed billing cycle normally are updated 4 days from the end of the billing cycle.

1.5 System Requirements

The DM/RA Application operates with the following Web browsers: Microsoft Internet Explorer versions 6.0 and higher. Users may access the application from the Internet at the following address:

Adobe Acrobat Reader and Microsoft Excel are required to export the RA reports to the PDF and Excel formats respectively.

1.6 Security

Application Security

Users are required to log in to the DM/RA Application for all operations using their Common Access Card (CAC) through the PCOLS Sign-on Referral System (SRS). All communication between the user's web browser and the DM/RA Application is encrypted. Each user session within the DM/RA Application will expire if the user is inactive for 30 minutes and the user will need to log in again to the application.

Data Security

All pages limit the amount of data users can see. Based on their assigned organization and hierarchical levels, users can only see the data related to the users that falls under their responsibility. The higher users are in the hierarchy, the more levels of data available to them for analysis. Users have access to data at their level and can drill-down to see lower levels of detail.

Some users have multiple assignments in the hierarchy. If a user has multiple assignments, then the user can switch between assignments within the DM/RA Application (see Section 4 for Navigation). A report can only be generated for a single organizational branch in the cardholder hierarchy. Users who are assigned to multiple organizations in the cardholder hierarchy can only access one of their organizations at a time.

All the content of the DM/RA Application is designated For Official Use Only (FOUO).

1.7 Technical Support

If the user needs help or support with DM/RA, please contact the DM/RA Help Desk:

- Toll-free Telephone: 1-800-376-7783
- OCONUS – DSN : 661-7307
- Direct Dial : 269-961-7307
- Email: dlacontactcenter@dla.mil

Formatted: Bullets and Numbering

DRAFT

2. DM/RA Users and Hierarchy

Access to the DM/RA Application varies by the user's hierarchy level and whether the user is in the Data Mining or the Risk Assessment applications. User titles designate a specific role for the user which is described in detail in Section 5.2 for Data Mining and Section 6.2 for Risk Assessment. The Hierarchy role titles are as follows (except for the Navy):

- Level 1 - DoD Purchase Card Program Management Office (PCPMO)
- Level 2 - Acquisition Executive Agent (Level 2)
- Level 3 - HCA Agent (Level 3)
- Level 4 - Agency/Organization Program Coordinator (A/OPC) and A/OPC Supervisor
- Level 5 - Approving/Billing Official (A/BO), A/BO Alternate and A/BO Supervisor

The Navy has an additional level in the user hierarchy:

- Level 1 - DoD Purchase Card Program Management Office (PCPMO)
- Level 2 - Acquisition Executive Agent (Level 2)
- Level 3 - HCA Agent (Level 3)
- Level 4 - High-Level A/OPC
- Level 5 - Agency/Organization Program Coordinator (A/OPC) and A/OPC Supervisor
- Level 6 - Approving/Billing Official (A/BO), A/BO Alternate and A/BO Supervisor

If a user is assigned to multiple roles, he/she can select which role's view of the DM/RA Application they will see on first log-in (detailed in Section 4.1), but at any time they can switch roles by clicking the "Select Role" link at the top right corner of every page.

DRAFT

3. Log-on Functions

3.1 Logging In

To log into DM/RA directly:

1. Insert the user's Common Access Card (CAC) into the card reader.
2. Enter the PIN for the user's CAC and click OK.
3. Open Internet Explorer and enter the following Web address:
4. Select the "Log On" button under "Data Mining/Risk Assessment (DM/RA)" in Figure 1.

To log into DM/RA from a Notification Email:

1. Click the DM/RA link in notification email received.
2. Insert the user's Common Access Card (CAC) into the card reader.
3. Enter the PIN for the user's CAC and click OK.
4. Select the "Log On" button under the "Data Mining/Risk Assessment (DM/RA)" in Figure 1.

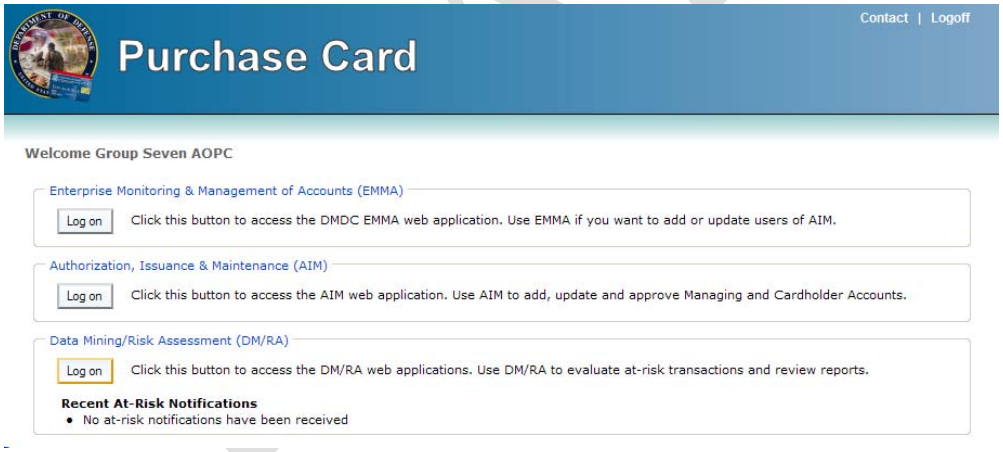


Figure 1: PCOLS Logon Page

4. Navigation

4.1 General Navigation

The Data Mining/Risk Assessment Application allows users to easily navigate through all its components. In the top right corner of every page is a "Help" link that takes users to the PCOLS website where users can download the DM/RA User Manual from the "Available For Download" section. In addition, throughout the DM Application are question mark "?" buttons next to links and questions which provide contextual help and guidance based on law, regulation and/or policies and procedures. Also located on the top right of every page is a "Contact" link which displays phone and email contact support (described in Section 1.7), a "Select Role" link which takes the user to the User Role Selection page, and a "Logoff" link which signs the user out of the application (example shown in Figure 2).

Users should use the "Go Back" link in the right corner to return to the previous page viewed. **Note: Users should not use the browser's back button as it may cause problems with the information displayed**. At any time, the user can also return to the main Case Statistics page by clicking the first level code on the page or the "Case Management" tab when on the Case Statistics Results page.

When users first arrive in the DM/RA Application, the user role needs to be selected by clicking the "Select" button (Figure 2) next to the desired role. Only users assigned to multiple hierarchies will have more than one option to select a specific role within a specific hierarchy. At any time, the user can change roles by clicking on the "Select Role" link in the upper right corner of every page which will take the user back to the User Role Selection page. The example in Figure 2 is what would be displayed for a user who is a Primary A/BO.

Important Note - The data presented within the figures is simulated data and does not reflect actual referred cases or the risk assessment of the Service/Organization or hierarchical level.

4.2 Data Mining Navigation

This section helps users navigate through the DM Application to access and view the Case Management screens and search all transaction within the application.

1. There are two tabs within the main "Data Mining" tab. The two tabs are:

   a. "Case Management"

   b. "Find Transactions"

Case Management Tab (detailed in Section 5.3)

2. Once a user role is selected, the main Case Statistics page is displayed within the "Case Management" tab.

3. For the DoD PCPMO user only, there is a choice of selection from the first column "Level" to drill-down by Service on the same Case Statistics page.

DRAFT

4. All users can click on any of the columns showing flagged transactions in their area of responsibility: new cases as "NEW", pending cases as "UNDER A/BO REVIEW", and closed cases as "CLOSED." Clicking on a link under the "Level" column takes the user to the Account Details page and clicking on the number of cases in each status column (New, Under A/BO Review, and Closed) takes the user to the Case Statistics Results page.
5. Once at the Account Details page, the user can click on the "View" or "Create" button at the end of each row to navigate to the Case Details page.
6. From the Case Details page, the user can click on the Account Number link to go back to the Account Details page.
7. The user can return to the Case Statistics page by clicking the first level code on the page or the "Case Management" tab when on the Case Statistics Results page.

Find Transactions Tab (detailed in Section 5.4)

8. Navigating from the "Find Transactions" tab follows the same general navigation steps as the "Case Management" tab.
9. Once users enter information into the Find Transactions filter and click the "Find" button, the transactions which fit the criteria are displayed.
10. Clicking on the "View" or "Create" buttons in the View column navigates the user to the Case Details page (follow from step 5), Only A/BO users can "Create: cases for review.
11. The user can return to the Case Statistics page by clicking the "Case Management" tab.

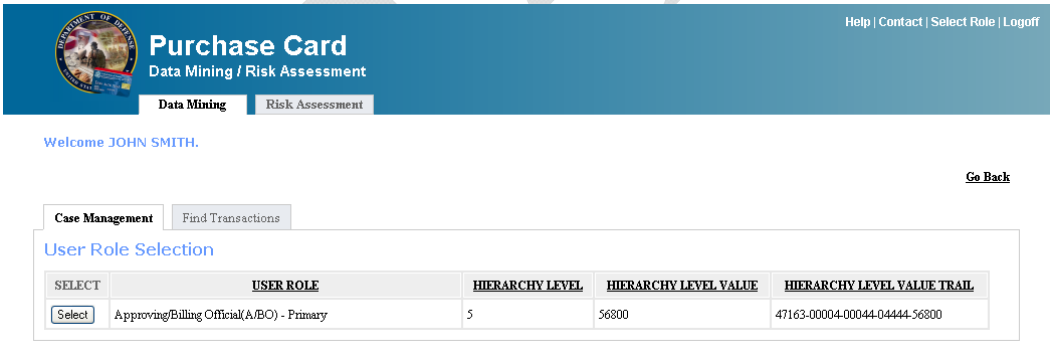


Figure 2: User Role Selection Page

4.3 Risk Assessment Navigation

This section helps users navigate through the RA Application to access and view the reports available within the application.

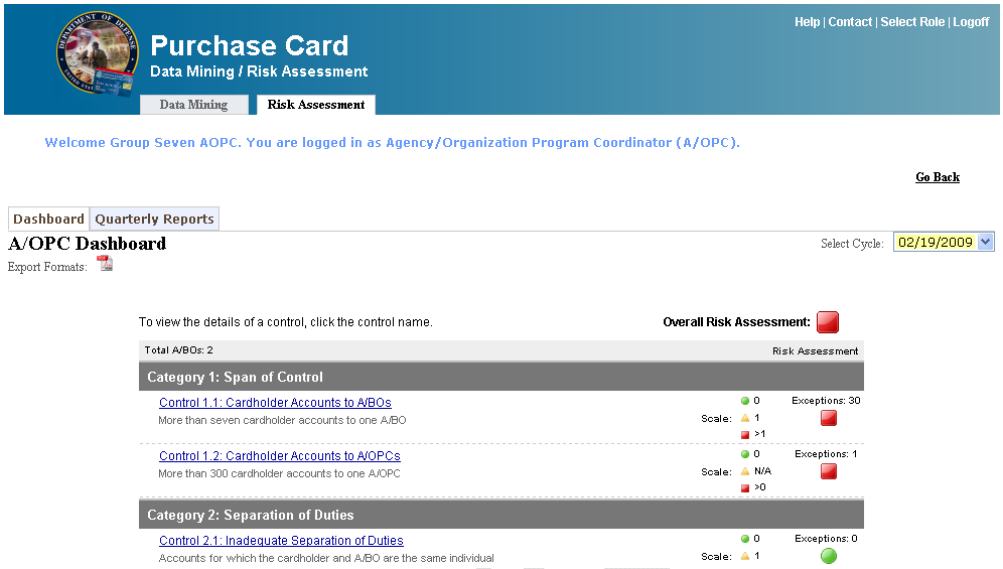


Figure 3: A/OPC User Dashboard

1. The user can access the RA Application by selecting the "Risk Assessment" tab.
2. Within the "Risk Assessment" tab, the user will see the "Dashboard" tab displaying the risk assessment dashboard (Figure 3).
3. A/OPC users and above may select the "Quarterly Reports" tab displaying a three-billing cycle, side-by-side snapshot of control exceptions.
4. Users may select "Help" in the upper right corner to access the DM/RA User Manual.
5. Users may select "Contact" in the upper right corner to display phone and email contact support information.

The details of each of the controls are described in subsequent sections. For example, the two controls under Category 1, Span of Control: Control 1.1 and Control 1.2, are described in Section 6.5, Viewing Control Reports and Section 6.6, Accessing Control Reports of this document.

5. Data Mining Application

5.1 Introduction

The DM Application is a powerful tool for users of the DoD Purchase Card Program that programmatically reviews 100% of the purchase card transactions and assigns a score. High risk transactions are subsequently referred for review by the A/BOs. In addition, a statistically based sample of random transactions is referred for review by the A/BOs. Through the use of the Case Manager Interview Process, the A/BO demonstrates that due diligence is exercised in the review of the referred transactions. Additionally, the interview process records information related to the data provided to support the validity of the purchase card transaction.

5.2 DM User Hierarchy

- **Level 1 - DoD Purchase Card Program Management Office (PCPMO)** user has read only access to review the transactions for the entire DoD Purchase Card Program and can add independent reviewer comments to the due diligence information and documentation provided by the A/BOs in the Case Management system.
- **Level 2 - Acquisition Executive Agent** has read only access to review the transactions at the Service/Organization level and can add independent reviewer comments to the due diligence information and documentation in the Case Management system.
- **Level 3 - HCA Agent** has read only access to review the transactions of all Approving/Billing Officials (A/BOs) under the Level 4 A/OPCs in their hierarchy and can add independent reviewer comments to the due diligence information and documentation in the Case Management system.
- **Level 4 - Agency/Organization Program Coordinators (A/OPCs)** have read only access to review the transactions of all A/BOs under the Level 5 A/OPCs in their hierarchy and can add independent reviewer comments to the due diligence information and documentation in the Case Management system. The A/OPC Supervisor has the same level of access and view of data as each of the A/OPCs under their purview.
- **Level 5 - Approving/Billing Officials (A/BOs)** use the Case Management system to review transactions of cardholders under their supervision that have been referred by the DM Application. A/BOs document their analysis of the transaction by answering a series of required questions based on specifics of the transaction type. The A/BO Alternate's view and use of the application is no different than that of the A/BO for which they are the alternate. The A/BO Supervisor has the same level of access and view of data as each of the A/BOs under their purview.

The Navy users' role and their access within the DM Application is an exception to the above hierarchy of all other Service/Organizations. The Navy is the only Service with the **High-Level A/OPC.**

- **Level 4 - High-Level A/OPCs** have read only access to review the transactions of all A/BOs in their hierarchy and can add independent reviewer comments to the due diligence information and documentation in the Case Management system.

DRAFT

This level is followed by **Level 5 - A/OPC** and **Level 6 - A/BO.**

5.3 Case Management

A/BOs are the first line users of the DM Application. The A/BO documents the review of all the cases that have been referred in the Case Management system.

A/BO Case Management

The referred cases are assigned for examination and displayed on the Case Statistics page. The A/OPC receives an email for high risk transactions, accesses the Case Management system and documents his/her independent review once the information is completed by the A/BO in the Case Management system. There is an escalation process if transactions are not reviewed in a timely manner and this will affect the risk assessment rating within the RA Dashboard. If the cases are not reviewed timely, the case can be escalated as high as the PCPMO. Information displayed under the Case Management tab can be filtered by cycle using the Cycle drop-down menu in the right corner of the screen (Figure 4 and Figure 5).

1. The first column "Level" in Figure 4 shows all the managing accounts that are under the purview of the A/BO.
2. The second column "NEW" shows the number of cases that have not yet been reviewed.
3. The third column "UNDER A/BO REVIEW" shows the number of cases under review (pending cases).
4. The fourth column "CLOSED" shows the number of dispositioned cases that have been reviewed and closed by the A/BO.

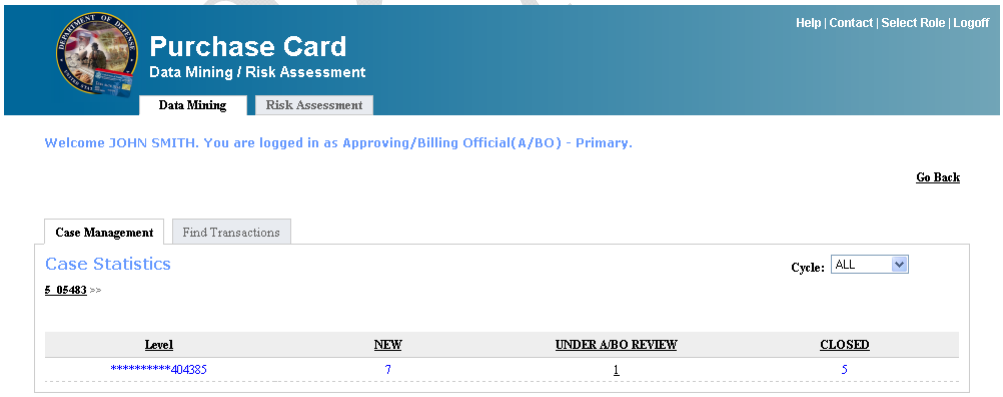


Figure 4: Case Management Tab - Case Statistics Page

Purchase Card Account Details

From the Case Statistics page, the user can navigate to the Account Details page by clicking on the level code links down through the hierarchy. Clicking on the number of cases in each status column (New, Under A/BO Review, and Closed) takes the user to the Case Statistics Results page.

- The Account Details page provides transaction history and Cardholder account information (Figure 5).

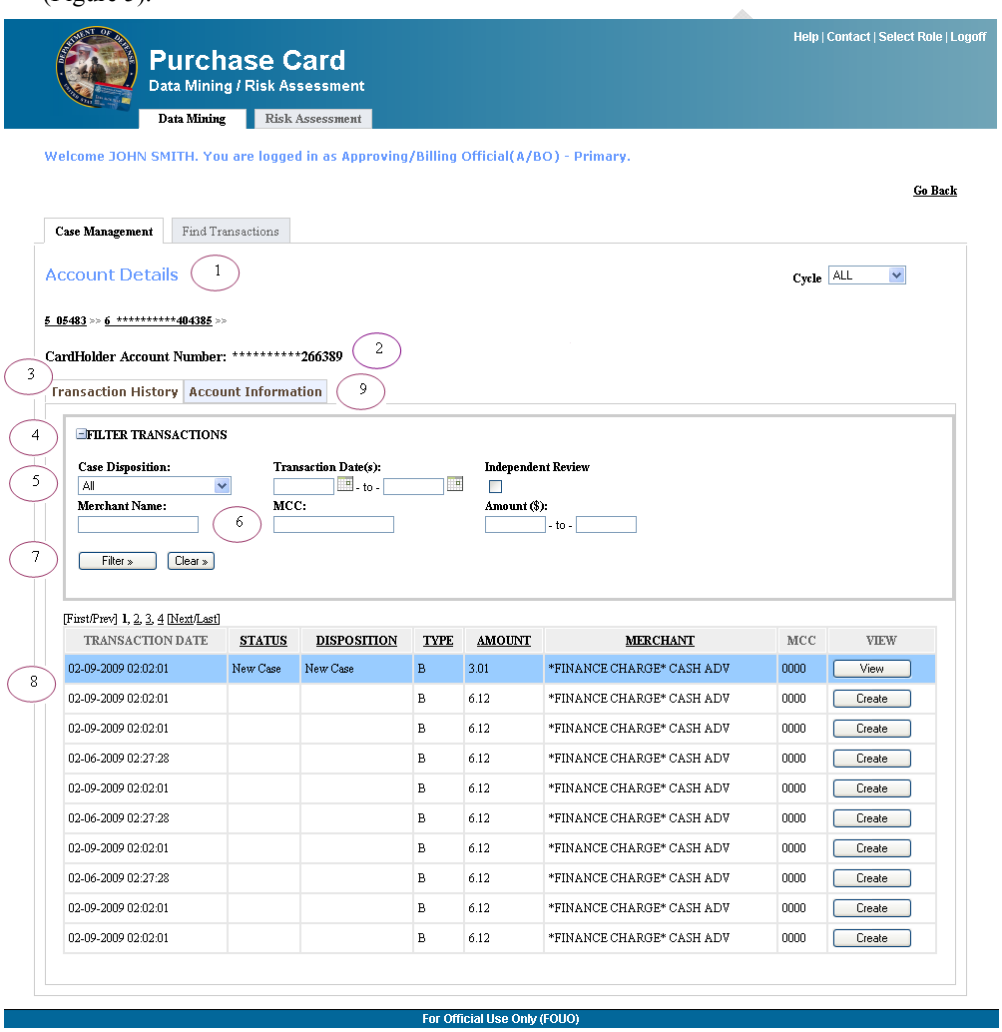


Figure 5: Account Details Page

1. At the top of the Account Details page (Figure 5) under the title are the hierarchy level codes.
2. The Cardholder account number is displayed indicating the account for which the account details are shown.
3. There are two tabs shown below the cardholder account number: "Transaction History" tab which is always the initial tab shown, and the "Account Information" tab.
4. Within the "Transaction History" tab, users can query transactions up to 18 months based on a number of variables under "Filter Transactions". Selecting the minimize button next to "Filter Transactions" hides the search parameters.
5. Filtering can be done by making one of the following case disposition drop-down selections: All, Under A/BO Review, Valid Transaction, Administrative Discrepancy, Misuse, Suspected Fraud, Abuse, Lost, or Stolen.
6. Results can also be filtered based on the Transaction Date(s) to be queried, Independent Review, Merchant Name, MCC, and Amount ($).
7. Once the filter has been determined, the user selects the "Filter" button to execute the search, and the "Clear" button to clear the entries on the form.
8. When results are displayed, the user may select a transaction from the "View" column by clicking on the "View" or "Create" buttons which brings up the Case Details page (Figure 7). Selecting the "View" which will be highlighted blue across the entire row or "Create" button will display the Case Details page. Only A/BO users can "Create" cases for review. For more details and guidance on initiating a case, see Section 5.4 Find Transactions.
9. In addition to the "Transition History" tab, users can view the "Account Information" tab. This page provides information on individual accounts.

Case Details

From the Account Details page, clicking on the "View" button will take users to the Case Details page. Here, the user can view detailed information associated with a transaction as well as any information entered during an A/BO's case review of the transaction. A/BOs also have an option of clicking the "Create" button to self initiate a case for transactions not flagged by the Data Mining Application. Once the case is initiated, the A/BO will answer a series of questions as described below in the Case Review Section (page 17).

- From the Case Details page, transactions can be viewed in two formats:
    i. All Grouped (Figure 6)
    ii. Summary (Figure 7)

DRAFT

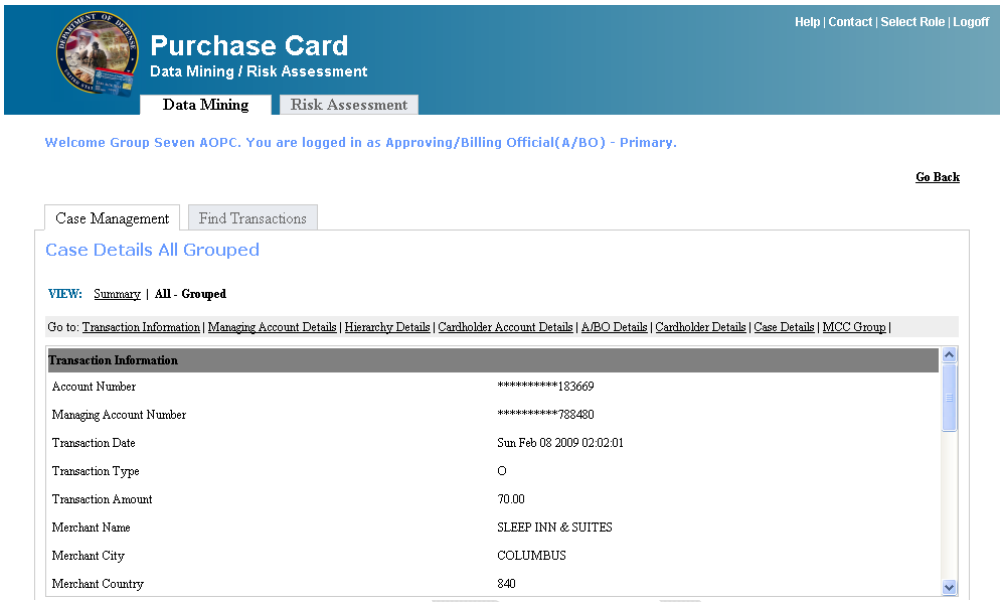


Figure 6: Case Details - All Grouped

All Grouped View

1. The All Grouped page (Figure 6) displays Transaction Information, Managing Account Details, Hierarchy Details, Cardholder Account Details, A/BO Details, Cardholder Details, Case Details, and MCC Group. Account detail categories vary by hierarchy level and data received from the banks.
2. The user may select the "Summary" link (Figure 8) at the top of the All Grouped Case Details page in order to answer the questions for the review and change the case status.

DRAFT

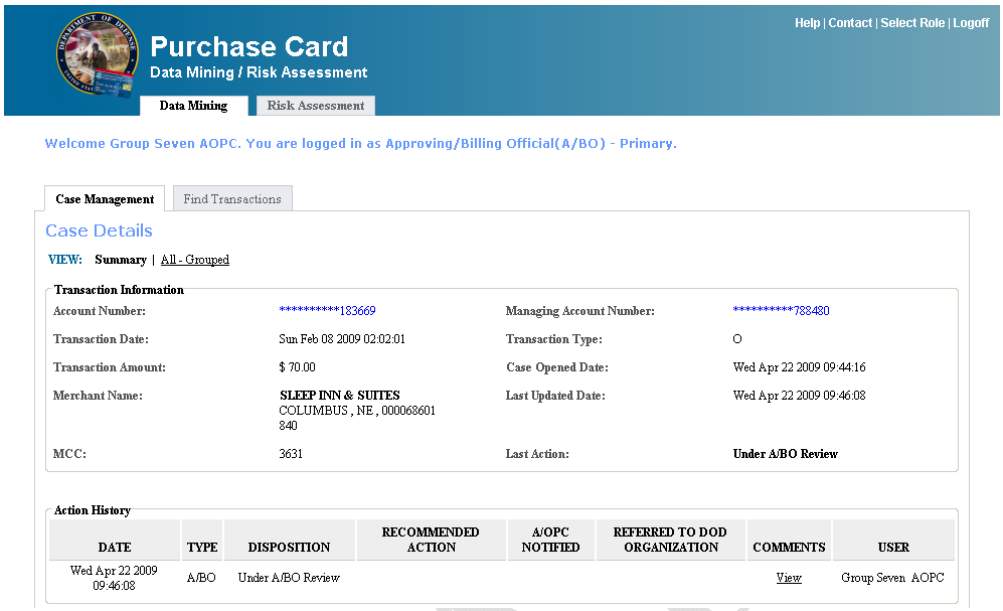


Figure 7: Case Details Page – Transaction Summary

Figure 8: Case Details Page - Review Button

Summary View

1. The first section displayed on the Case Details page in Summary view (Figure 7) is the "Transaction Information" section containing the Account Number, Managing Account Number, Transaction Date, Transaction Type, Transaction Amount, Case Opened Date, Last Updated Date, Merchant Name, MCC, and Last Action.
2. The "Action History" section shows the Date, Type, Disposition, Recommended Action, A/OPC Notified, Referred to DOD Organization, Comments, and User. Under the Comments column the user can select "View" to see comments made by the specific user.
3. The user's first action in the Case Details page is to describe the product or service acquired (Figure 8.1). This is requested when the field is not pre-populated with level three data from the banks. A/BO users must be as specific as possible.

4. The field associated with the question regarding the use of convenience checks is automatically populated with the data provided by the banks for the transaction. The additional questions which follow in the "Case Review" section will differ based on how the purchase was made. These questions include nine common questions and three additional ones specific to convenience checks.

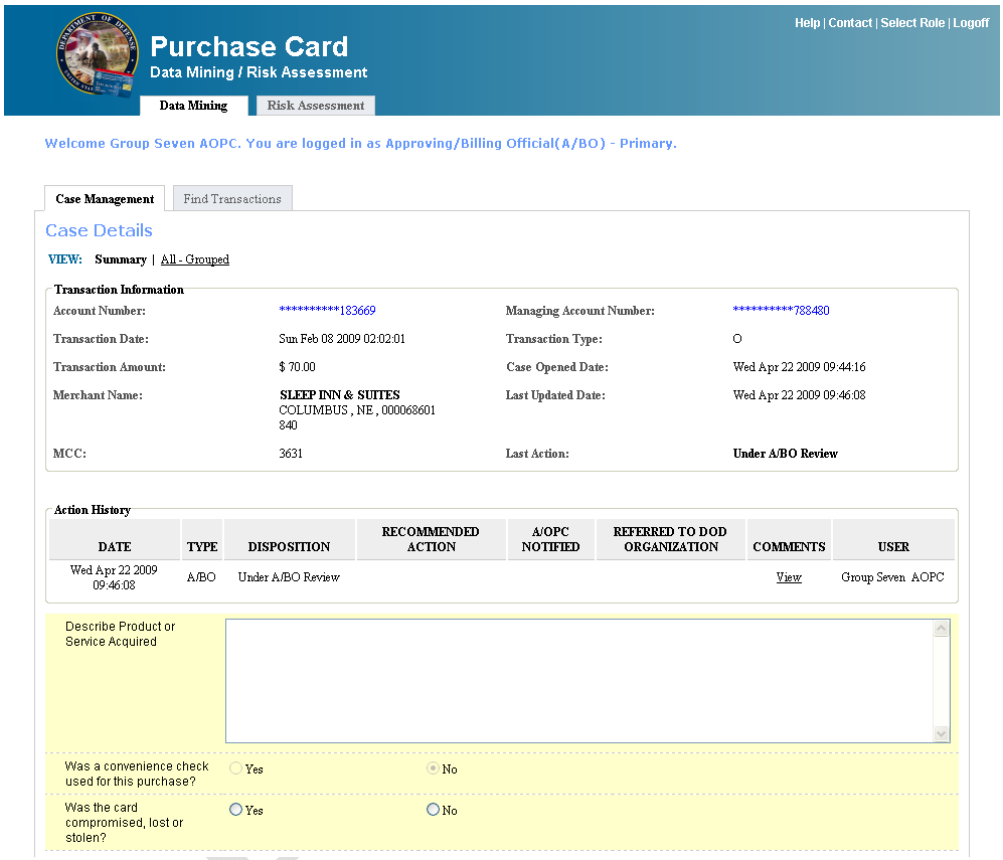


Figure 8.1: Case Details Page - Action History Section

5. The user must answer whether the card was compromised, lost or stolen (Figure 8.1). If the answer is "Yes", the A/BO user does not answer further questions. Instead, the user goes to the "Case Disposition" section (Figure 9) and from the Case Disposition drop-down menu, selects "Lost" or "Stolen" and must notify the bank and their supervisor.

6. If the card was not lost, or stolen, the user must answer all the questions under the "Case Review" section (Figure 8.2 or Figure 8.3 depending on if a convenience check was used for the purchase). For further guidance on how to answer these questions, click on the circular blue question mark "?" buttons next to each question.

7. The questions can be answered as "Yes or "No" by selecting the radio buttons and when a question doesn't pertain to the transaction being reviewed, there is an option for N/A. Every question must have an answer. Note that a yes or no response may trigger additional questions in a drop-down menu displayed to the right of the question. For example, answering "Yes" to "Was there adequate source documentation?" will trigger a list from which the user selects specific documents provided. Multiple selections may be made by holding down the "Ctrl' key.

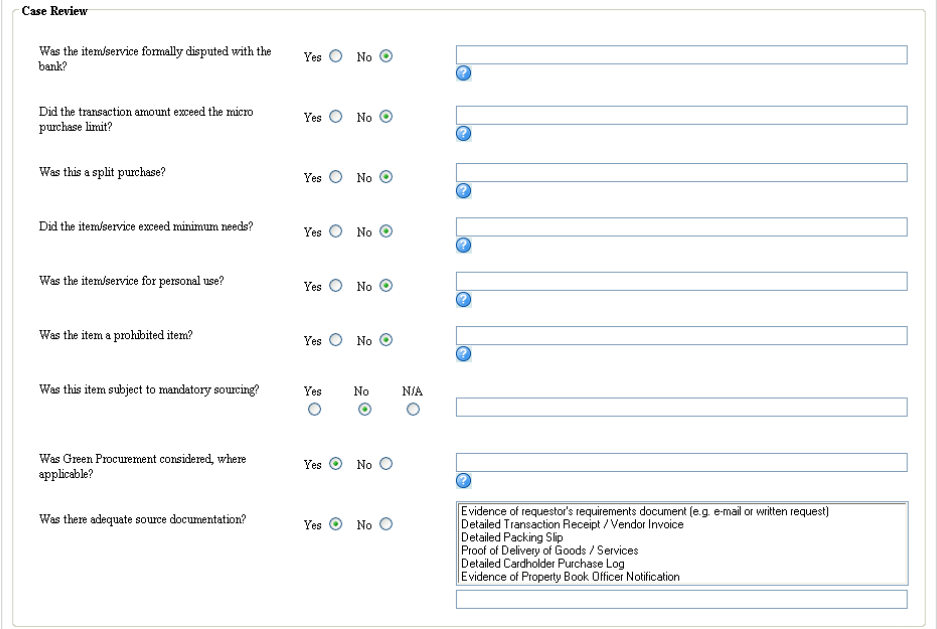


Figure 8.2: Case Details Page - Case Review Section

Case Review Section

Based on whether or not a convenience check was used for the transaction ("Yes" or "No"), the user answers a series of questions listed below. Note that answers to these questions will affect the applicable choices that will be available in the "Case Disposition" section for the Case Disposition drop-down menu.

For traditional purchases, the user must answer the following nine questions:

1. "Was the item/service formally disputed with the bank?" - The banks which issue the government credit cards have formal dispute and resolution procedures for transactions that a cardholder questions. The user must select "Yes" or "No" and may add additional information and details in the "Remarks" field. If "Yes" is selected, all the remaining questions will be grayed out. The cardholder has 60 days from the date of the billing statement to dispute a transaction and if a resolution cannot be reached with the merchant it is their responsibility to initiate a dispute with the issuing bank. Additional guidance can be found by clicking on the blue "?" button.

2. "Did the transaction amount exceed the micro purchase limit?" - The micro purchase threshold is established in the Federal Acquisition Regulation (FAR) and set by Congress as the maximum amount that can be charged on a credit card for a single transaction for supplies or services. The user must select "Yes" or "No" and may add additional information and details in the "Remarks" field. If "Yes" is selected, a drop-down menu will appear and the user must make a selection from the following options: DAPS Order, Task or Delivery Order (BPA on an existing contract), Training (allowed to $25,000), or Other (Specify). If this transaction represents a contract payment and does not fall under the available options, select Other and provide details in the comments field. For the acquisition of services subject to the Service Contract Act the threshold is $2,500. Additional guidance can be found by clicking on the blue "?" button.
3. "Was this a split purchase?" - A purchase is considered split purchase when a cardholder intentionally divides the purchase into units less than the micro purchase limit in order to circumvent the single transaction maximum. The user must select "Yes" or "No" and may add additional information and details in the "Remarks" field. No government purchase cardholder may fragment/split purchases that exceed the limit or threshold, as means to use the purchase card. Additional guidance can be found by clicking on the blue "?" button.
4. "Did the item/service exceed minimum needs?" - A good or service purchased should aim to meet the minimum needs of the desired use and not exceed other similar or like goods or services. The user must select "Yes" or "No" and may add additional information and details in the "Remarks" field. It is the responsibility of the cardholder to ensure purchases are proper, legal, and reasonable and would not qualify as misuse and abusive, fraudulent and improper purchases. Additional guidance can be found by clicking on the blue "?" button.
5. "Was the item/service for personal use?" - Personal use means the item/service was not purchased exclusively for government activities. The user must select "Yes" or "No" and may add additional information and details in the "Remarks" field. If "Yes" is selected, a drop-down menu will appear and the user must make a selection from the following options: Accidental Use: Restitution Made, Accidental Use: No Restitution Made, Intentional: Restitution Made, Intentional: No Restitution Made, Other (Specify). Use of a government charge card for other than official government purposes is characterized as misuse. Additional guidance can be found by clicking on the blue "?" button.
6. "Was the item a prohibited item?" - Prohibited items are specified in the FAR as items that would never be used or needed as part of typical government activity. The user must select "Yes" or "No" and may add additional information and details in the "Remarks" field. If "Yes" is selected, a drop-down menu will appear and the user must make a selection from the following options: Written Waiver in accordance with FAR was obtained, No waiver was obtained. Additional guidance can be found by clicking on the blue "?" button.
7. "Was this item subject to mandatory sourcing?"- Mandatory sourcing requires the federal government to purchase certain specific products if they can meet the required needs of the government at a competitive rate. The user must select "Yes", "No", or "N/A" and may add additional information and details in the "Remarks" field. If "Yes" is selected, a

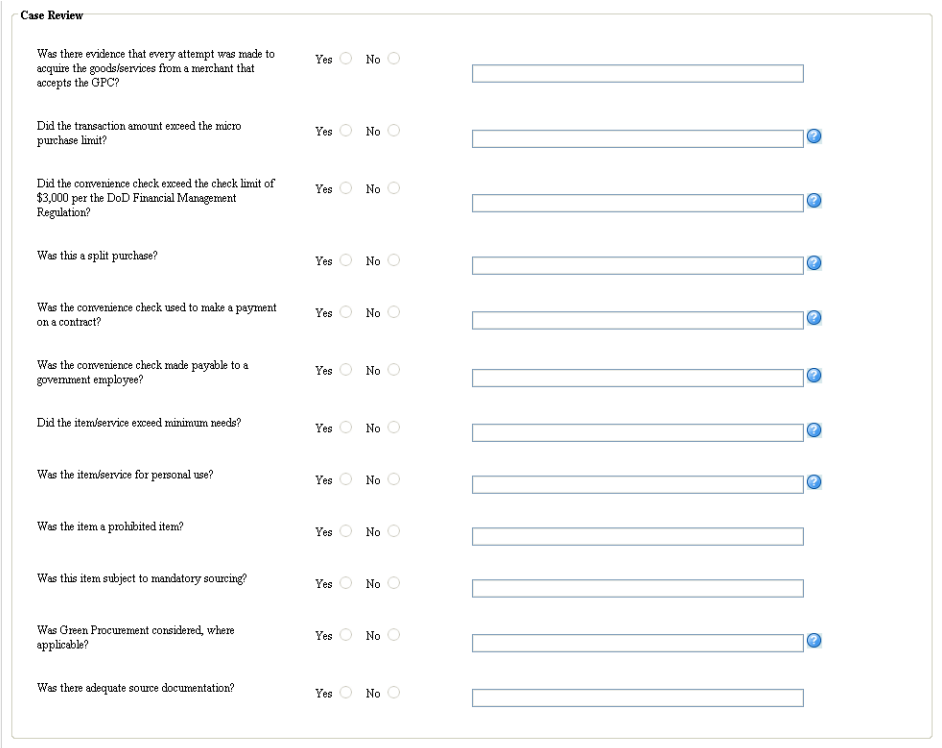
DRAFT

drop-down menu will appear and the user must make a selection from the following options: Mandatory Source Used, Mandatory Source Not Used - Item not available in required time frame, Mandatory Source Not Used - Other, Mandatory Source Not Used - Written Waiver Obtained, Mandatory Source Not Used - No Written Waiver Obtained.

8. "Was Green Procurement considered, where applicable?" - Green procurement is the purchase of environmentally preferable products and services that reduce resource consumption and waste generation. The user must select "Yes" or "No" and may add additional information and details in the "Remarks" field. Additional guidance can be found by clicking on the blue "?" button.

9. "Was there adequate source documentation?" - The user must select "Yes" or "No". If "Yes" is selected a drop-down menu will appear and the user may choose from the following six options. The user should select all choices which are applicable. To select more than one choice from the drop-down menu, the user must hold the control key while clicking on each of the selections. The six choices are as follows:
   - "Evidence of requester's requirements document (e.g. email or written request)" - A requirements document outlines the transactions purpose and what need it is expected to meet.
   - "Detailed Transaction Receipt/Vendor Invoice" - A receipt/vendor invoice shows the exact purchase amount of the transaction. These documents should include evidence of independent verification and details of the transaction on an invoice or receipt.
   - "Detailed Packing Slip" - A packing slip is a document that accompanies items shipped through the mail and outlines the content of the package and purchase details.
   - "Proof of Delivery of Goods/Services" - Proof of delivery establishes that the recipient has received the specified contents sent by the sender.
   - "Detailed Cardholder Purchase Log" - A cardholder purchase log is a record of purchases with associated transaction details. The DoD Charge Card Guidebook identifies as a mandatory management control the maintenance of a purchase log including a description, the merchant, the date purchased, the name of the recipient of the item, and the total amount.
   - "Evidence of Property Book Officer Notification" - The property book officer manages the records for all leased, loaned and borrowed equipment under their responsibility.

DRAFT



Case Review

Was there evidence that every attempt was made to acquire the goods/services from a merchant that accepts the GPC?	Yes ○ No ○	
Did the transaction amount exceed the micro purchase limit?	Yes ○ No ○	
Did the convenience check exceed the check limit of $3,000 per the DoD Financial Management Regulation?	Yes ○ No ○	
Was this a split purchase?	Yes ○ No ○	
Was the convenience check used to make a payment on a contract?	Yes ○ No ○	
Was the convenience check made payable to a government employee?	Yes ○ No ○	
Did the item/service exceed minimum needs?	Yes ○ No ○	
Was the item/service for personal use?	Yes ○ No ○	
Was the item a prohibited item?	Yes ○ No ○	
Was this item subject to mandatory sourcing?	Yes ○ No ○	
Was Green Procurement considered, where applicable?	Yes ○ No ○	
Was there adequate source documentation?	Yes ○ No ○	

Figure 8.3: Case Details Page - Case Review Section: Convenience Check Used

If a convenience check WAS used for the purchase the user must answer the following twelve questions:

1. "Was there evidence that every attempt was made to acquire the goods/services from a merchant that accepts the GPC?" - Convenience checks and foreign drafts provide a purchasing alternative to normal GPC transactions and formal contracting, and they are to be used only when the use of the purchase card is not possible. The user must select "Yes" or "No" and may add additional information and details in the "Remarks" field.
2. "Did the transaction amount exceed the micro purchase limit?" - The micro purchase threshold is established in the Federal Acquisition Regulation (FAR) and set by Congress as the maximum amount that can be charged on a credit card for a single transaction for supplies or services. The user must select "Yes" or "No" and may add additional information and details in the "Remarks" field. If "Yes" is selected, a drop-down menu will appear and the user must make a selection from the following options: DAPS Order, Task or Delivery Order (BPA on an existing contract), Training (allowed to $25,000), or Other (Specify). If this transaction represents a contract payment and does not fall under

the available options, select Other and provide details in the comments field. For the acquisition of services subject to the Service Contract Act the threshold is $2,500. Additional guidance can be found by clicking on the blue "?" button.

3. "Did the convenience check exceed the check limit of $3,000 per the DoD Financial Management Regulation?" - The total dollar value of convenience check purchases should not be greater than the specified limit. The user must select "Yes" or "No" and may add additional information and details in the "Remarks" field. Additional guidance can be found by clicking on the blue "?" button.
4. "Was this a split purchase?" - A split purchase is when a cardholder intentionally divides the purchase into units less than the micro purchase limit in order to circumvent the single transaction maximum. The user must select "Yes" or "No" and may add additional information and details in the "Remarks" field. No government purchase cardholder may fragment/split purchases that exceed the limit or threshold, as means to use the purchase card. Additional guidance can be found by clicking on the blue "?" button.
5. "Was the convenience check used to make a payment on a contract?" - A contract is a written agreement on behalf of the Government with an agreed upon delivery and payment for goods or services. The user must select "Yes" or "No" and may add additional information and details in the "Remarks" field. Additional guidance can be found by clicking on the blue "?" button.
6. "Was the convenience check made payable to a government employee?" - A government employee is an individual engaged in work on behalf of the Government. The user must confirm if the check is written out to an individual. The user must select "Yes" or "No" and may add additional information and details in the "Remarks" field. Additional guidance can be found by clicking on the blue "?" button.
7. "Did the item/service exceed minimum needs?" - A good or service purchased should aim to meet the minimum needs of the desired use and not exceed other similar or like goods or services. The user must select "Yes" or "No" and may add additional information and details in the "Remarks" field. It is the responsibility of the cardholder to ensure purchases are proper, legal, and reasonable and would not qualify as misuse and abusive, fraudulent and improper purchases. Additional guidance can be found by clicking on the blue "?" button.
8. "Was the item/service for personal use?" - Personal use means the item/service was not purchased exclusively for government activities. The user must select "Yes" or "No" and may add additional information and details in the "Remarks" field. If "Yes" is selected, a drop-down menu will appear and the user must make a selection from the following options: Accidental Use: Restitution Made, Accidental Use: No Restitution Made, Intentional: Restitution Made, Intentional: No Restitution Made, Other (Specify). Use of a government charge card for other than official government purposes is characterized as misuse. Additional guidance can be found by clicking on the blue "?" button.
9. "Was the item a prohibited item?" - Prohibited items are specified in the FAR as items that would never be used or needed as part of typical government activity. The user must select "Yes" or "No" and may add additional information and details in the "Remarks" field. If "Yes" is selected, a drop-down menu will appear and the user must make a

DRAFT

selection from the following options: Written Waiver in accordance with FAR was obtained, No waiver was obtained. Additional guidance can be found by clicking on the blue "?" button.

10. "Was this item subject to mandatory sourcing?" - Mandatory sourcing requires the federal government to purchase certain specific products if they can meet the required needs of the government at a competitive rate. The user must select "Yes", "No", or "N/A" and may add additional information and details in the "Remarks" field. If "Yes" is selected, a drop-down menu will appear and the user must make a selection from the following options: Mandatory Source Used, Mandatory Source Not Used - Item not available in required time frame, Mandatory Source Not Used - Other, Mandatory Source Not Used - Written Waiver Obtained, Mandatory Source Not Used - No Written Waiver Obtained.
11. "Was Green Procurement considered, where applicable?" - Green procurement is the purchase of environmentally preferable products and services that reduce resource consumption and waste generation. The user must select "Yes" or "No" and may add additional information and details in the "Remarks" field. Additional guidance can be found by clicking on the blue "?" button.
12. "Was there adequate source documentation?" - The user must select "Yes" or "No". If "Yes" is selected a drop-down menu will appear and the user may choose from the following six options. The user should select all choices which are applicable. To select more than one choice from the drop-down menu, the user must hold the control key while clicking on each of the selections. The six choices are as follows:
    - "Evidence of requester's requirements document (e.g. email or written request)" - A requirements document outlines the transactions purpose and what need it is expected to meet.
    - "Detailed Transaction Receipt/Vendor Invoice" - A receipt/vendor invoice shows the exact purchase amount of the transaction. These documents should include evidence of independent verification and details of the transaction on an invoice or receipt.
    - "Detailed Packing Slip" - A packing slip is a document that accompanies items shipped through the mail and outlines the content of the package and purchase details.
    - "Proof of Delivery of Goods/Services" - Proof of delivery establishes that the recipient has received the specified contents sent by the sender.
    - "Detailed Cardholder Purchase Log" - A cardholder purchase log is a record of purchases with associated transaction details. The DoD Charge Card Guidebook identifies as a mandatory management control the maintenance of a purchase log including a description, the merchant, the date purchased, the name of the recipient of the item, and the total amount.
    - "Evidence of Property Book Officer Notification" - The property book officer manages the records for all leased, loaned and borrowed equipment under their responsibility.

DRAFT

Case Disposition Section

1. The A/OPC and above users in the hierarchy have access to the A/BO's analysis and can provide comments which are documented as part of the case.
2. Once the "Case Review" section is filled out, the user has to complete the "Case Disposition" section (Figure 9). For this, the user must select from the status choices that reflect the decision on the case. The available choices are as follows:
    a. Under A/BO Review - This case disposition reflects that the A/BO is still gathering information for his/her review which has not been completed. When this choice is selected an additional drop-down menu is displayed with the option to select: Pending Documentation or Waiting Merchant Verification.
    b. Valid Transaction - This case disposition reflects the judgment by the A/BO that the transaction related to the case being examined is legitimate.
    c. Administrative Discrepancy - This case disposition reflects the judgment by the A/BO that the transaction issue is clerical. When this choice is selected an additional drop-down menu is displayed with the option to select a recommended disciplinary action: Counseling, Refresher Training, Admonishment, Reprimand, NonJudicial Punishment (military only), Court Martial (military only), Administrative Separation, Suspension, Removal, or Other.
    d. Misuse - This case disposition reflects the judgment by the A/BO that the government purchase card transactions are intended for government use, but are not permitted by law, regulation, or organization policy. When this choice is selected an additional drop-down menu is displayed with the option to select a recommended disciplinary action: Counseling, Refresher Training, Admonishment, Reprimand, NonJudicial Punishment (military only), Court Martial (military only), Administrative Separation, Suspension, Removal, or Other. In the case of misuse, the A/OPC should be notified by the A/BO and the box under the Disciplinary action should be checked. Note: Although A/BO users can select that the A/OPC has been notified, the system does not generate the notification. Instead, the A/BO must do this separately.
    e. Suspected Fraud - This case disposition reflects the judgment by the A/BO that the use of the government purchase card to acquire goods or services was unauthorized and intended for personal use or gain constituting a fraud against the government. When this choice is selected an additional drop-down menu is displayed with the option to select a recommended disciplinary action: Counseling, Refresher Training, Admonishment, Reprimand, NonJudicial Punishment (military only), Court Martial (military only), Administrative Separation, Suspension, Removal, or Other. In the case of suspected fraud, the A/OPC should be notified by the A/BO and the checkbox under the recommended disciplinary action drop-down should be checked. Note: Although A/BO users can select that the A/OPC has been notified, the system does not generate the notification. Instead, the A/BO must do this separately. Also note that the transaction should be referred to the appropriate DoD organization and the associated checkbox should be checked when that has been accomplished.

DRAFT

f. Abuse - This case disposition reflects the judgment by the A/BO that the Purchases of authorized goods or services at terms (e.g., price, quantity) are excessive, for a questionable government need, or both. When this choice is selected an additional drop-down menu is displayed with the option to select a recommended disciplinary action: Counseling, Refresher Training, Admonishment, Reprimand, NonJudicial Punishment (military only), Court Martial (military only), Administrative Separation, Suspension, Removal, or Other. Note: Although A/BO users can select that the A/OPC has been notified, the system does not generate the notification. Instead, the A/BO must do this separately.

g. Lost - This case disposition reflects that the purchase card was lost or misplaced and is either no longer in the possession of the cardholder or the information has been compromised.

h. Stolen - This case disposition reflects that the purchase card was stolen from the cardholder and the information has been compromised.

3. Additional information may be entered into the Notes field including any dates or additional relevant information. Note: Although A/BO users can select that the A/OPC has been notified, the system does not generate the notification. Instead, the A/BO must do this separately.

4. Select the "Save" button to save the information. Selecting the "Cancel" button will remove any changes made and return the user to the "Case Management" tab (Figure 4).

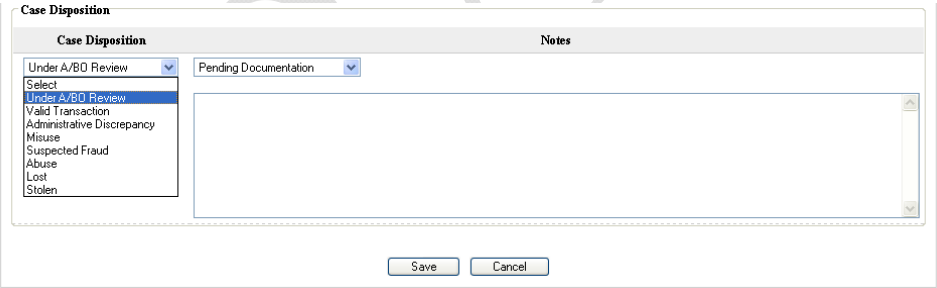


Figure 9: Case Details Page - Case Disposition Section

Independent Reviewers' Case Management

A/OPCs and other authorized users may conduct case reviews after the A/BO completes a review of the case. All A/OPCs and above have read only access to review the transactions for the DoD Purchase Card Program and can add independent reviewer comments to the due diligence information and documentation provided by the A/BOs.

1. Navigate to the Case Details page of a specific case.
2. Under the "Action History" section (Figure 10) there is an "Add Independent Review" button. Make sure the page is in summary view.
3. The independent reviewer can see everything the A/BO has completed including the "Case Disposition" and "Notes" entered by the A/BO. After reviewing the A/BO's case analysis, the independent reviewer clicks the "Add Independent Review" button and completes the information in the popup box displayed documenting his/her assessment of the A/BO's determination. The user has the following choices for case disposition: Under A/BO Review, Valid Transaction, Administrative Discrepancy, Misuse, Suspected Fraud, Abuse, Lost, or Stolen. Users must include any discrepancies or justification in the comments field. If the independent reviewer disagrees with the A/BO assessment, the A/BO should be contacted to resolve the discrepancy.

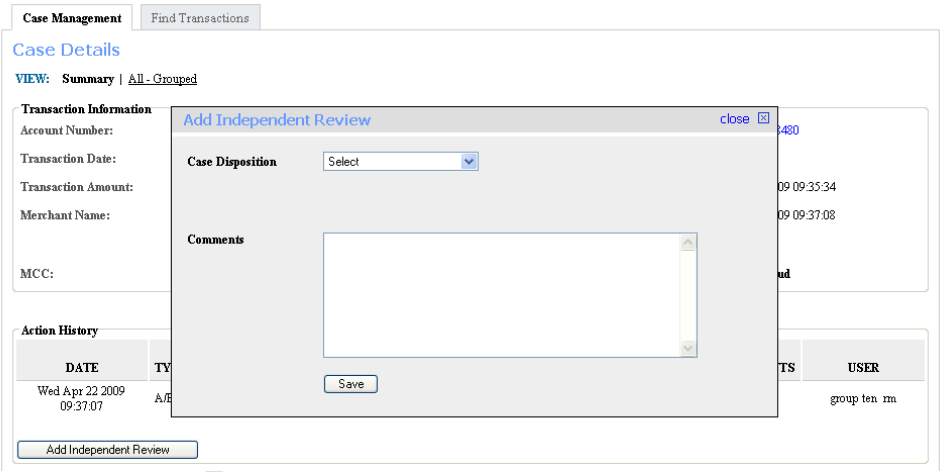


Figure 10: Case Details Page - Independent Review Popup

5.4 Find Transactions

The "Find Transactions" tab is the second tab displayed within the main Data Mining tab (Figure 11.1). Users may query all transactions by Account Type, Case Disposition, Transaction Date(s), Independent Review, Merchant Name, MCC, and/or Amount ($). While the information displayed in the Case Management tab shows transactions that have been referred by the application, it is possible for users to search through all transactions to review the data, or create additional cases which have not been identified for review by the Data Mining Application.

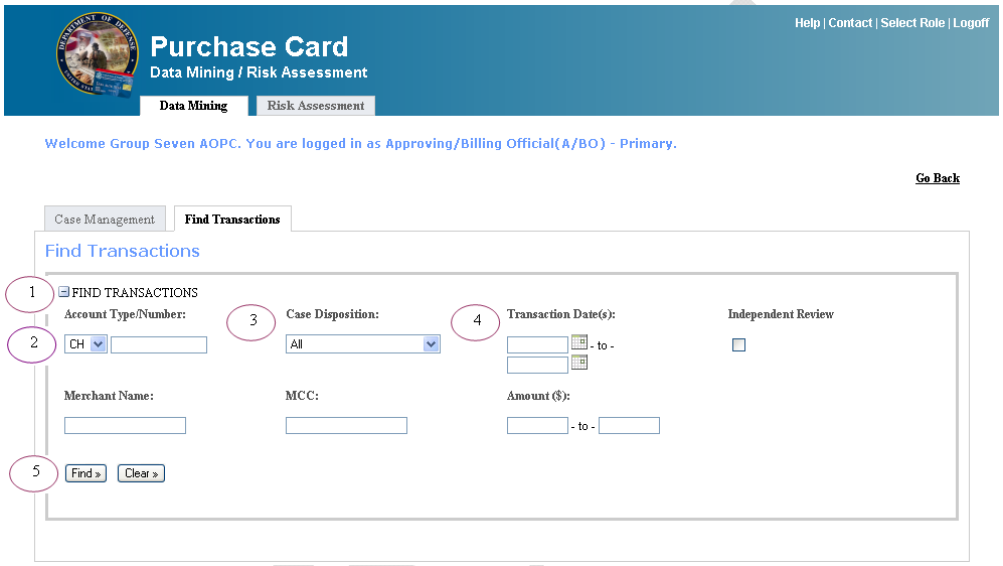


Figure 11.1: Find Transactions - Search

1. Users can find transaction histories based on a number of variables under "Find Transactions". Selecting the minimize button next to "Find Transactions" hides the search.
2. The account type can be queried by Cardholder or Managing Account selecting CH or MA respectively from the drop-down choices.
3. Filtering can also be done by making one of the following case disposition selections: All, Under A/BO Review, Valid Transaction, Administrative Discrepancy, Misuse, Suspected Fraud, Abuse, Lost, or Stolen.
4. Additional filtering can be done based on the beginning and ending Transaction Date(s) to be queried, If an Independent Review was done, Merchant Name, MCC, and Amount ($).
5. Once information has been entered into the filter, the user must click the "Find" button to execute the search. Clicking the "Clear" button will clear the entries on the form. If the search is too large, the system will display a warning message requesting that the user refine the search.
6. Results will be displayed by Transaction Date, Status, Disposition, Type, Amount, Merchant, MCC, and View. Note: the information can be sorted by clicking on the column names.

7. When results are displayed, the user may view a transaction by clicking on the "View" or "Create" buttons under the "View" column. Clicking the "View" or "Create" button will display the Case Details page for the selected transaction. Only A/BO users can "Create" cases for review. For more details and guidance on initiating a case, see Section 5.3 Case Management.

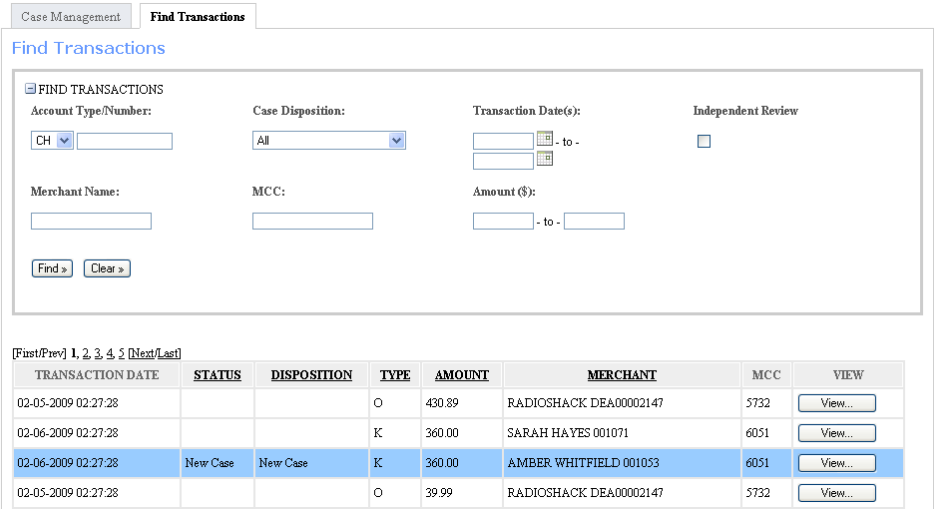


Figure 11.2: Find Transactions - Results

Self Initiating Cases

Only A/BO users can self initiate additional cases for transactions in the system. This can be done from both the “Find Transactions” tab (Figure 11.2) and the “Account Details” page under the “Case Management” tab (Figure 5).

A self initiated case can be created from the “Find Transactions” tab (Figure 11.2). Once the user has entered in search criteria, the results are displayed. In addition, from the "Case Management" tab (Figure 5), a user can drill-down to the "Account Details" page to see all the transactions displayed.

In both cases, the rows that are highlighted in blue are transactions which have already been flagged by the system. To create a new case on a transaction that hasn’t been flagged, click the “Create” button in the "View" column. The user can also click the “View” button on Blue Highlighted rows to see the Case Details page for transactions that have already been flagged.

6. Risk Assessment Application

6.1 Introduction

The RA Application is a powerful new tool that uses internal controls and measures coupled with results from the DM Application to quantify and report the inherent risk of DoD organizations' purchase card programs. All this information is clearly displayed in the RA Application through organizational dashboards that assess the risks associated with the organization's purchase card program.

6.2 RA User Hierarchy

The RA Application has a hierarchical structure for drilling down into the data to analyze risk. Report access and content varies by the user's hierarchy level. The users' role and their access within the RA Application are described below:

- **Level 1 - DoD PCPMO** users monitor risk for the entire DoD Purchase Card Program with access to all levels of data.
- **Level 2 - Acquisition Executive Agents** monitor risk of all the Level 3s and below in their purchase card hierarchy. They have access to all levels of data within their Service/Organization and can drill-down to all data within that Service/Organization.
- **Level 3 - HCA Agents** monitor risk of all Level 4s and below in their purchase card hierarchy. The HCA Agents have access to drill-down to the data of the A/OPCs, (High-Level A/OPCs for the Navy), and A/BOs under their responsibility.
- **Level 4 - A/OPCs** monitor risk of all Level 5s and below in their purchase card hierarchy. They have access to drill-down and monitor data of the A/BOs and A/OPCs under their responsibility. The A/OPC Supervisor has the same level of access and view of data as each of the A/OPCs under their purview.
- **Level 5 - A/BOs** monitor risk of cardholders in their purchase card hierarchy. They have access to the data of all cardholders under their responsibility. The A/BO Alternate's view and use of the application is no different than that of the A/BO for which they are the alternate. The A/BO Supervisor has the same level of access and view of data as each of the A/BOs under their purview.

The Navy users' role and their access within the DM Application are an exception to the above hierarchy. The Navy is the only Service with **High-Level A/OPCs.**

- **Level 4 - High-Level A/OPCs** monitor risk of all A/BOs and below in their purchase card hierarchy. The Navy High-Level A/OPC users have access to drill-down and monitor data of the A/BOs and A/OPCs under their responsibility.

This level is followed by **Level 5 - A/OPC** and **Level 6 - A/BO**

DRAFT

6.3 RA Controls

The RA Application assesses risk using twelve controls. Each of the twelve controls fall under one of five categories listed below:

1. Span of Control
2. Separation of Duties
3. Authorization Controls
4. Card Status
5. Transaction Review Controls

Figure 12, below, summarizes each control within each category.

Category	Control	Exception Description
1: Span of Control	Control 1.1: Cardholder Accounts to A/BOs	More than seven Cardholder accounts to one Approving/Billing Official
	Control 1.2: Cardholder Accounts to A/OPCs	More than 300 Cardholder accounts to one A/OPC
2: Separation of Duties	Control 2.1: Inadequate Separation of Duties	Accounts for which the Cardholder and A/BO are the same individual
3: Authorization Controls	Control 3.1: Spending Ratio - Underutilized Credit Limits	Accounts for which the six cycle spend average is less than 70% of the average cycle credit limit
	Control 3.2: Single Merchant Spending	Accounts that have at least ten transactions and an 80% or greater spending percentage at one merchant
4: Card Status	Control 4.1: Delinquent Accounts	Managing Accounts delinquent for 30+ days
	Control 4.2: Account Usage	Accounts that have been inactive for six cycles or have never been used (Excludes newly issued cards 60 days from the end of the billing cycle)
	Control 4.3: Lost/Stolen Cards	Accounts that have greater than one lost/stolen card(s) in the last 12 cycles
5: Transaction Review Controls	Control 5.1: Average Cycle Transactions Reviewed	Higher than average number of transactions (>100) per cycle reviewed by the A/BO, based on three cycles of data
	Control 5.2: A/BO Response Rate	A/BO failure to initiate case review in Case Management for flagged transactions within 10 days
	Control 5.3: Flagged Transaction Determination	Flagged transactions determined to be other than valid in Case Management (Misuse/Abuse/Suspected Fraud)
	Control 5.4: Convenience Check Amounts	Convenience Checks over $3,000

Figure 12: RA Controls

DRAFT

6.4 RA Dashboards

RA Dashboards are based on the user's hierarchy level (described in Section 6.2). The dashboards by hierarchy levels of RA users are listed below:

1. **PCPMO Dashboard -** Used to monitor risk of the DoD Purchase Card Program. This dashboard provides a side-by-side comparison of the risk assessments for all Services/Organizations. This dashboard has drill-down capability to all levels of the hierarchy.
2. **Acquisition Executive Agent (Level 2) Dashboard -** Used to monitor risk at the Service/Organization level: Navy, Army, Air Force, and Other Defense Agencies. This dashboard provides drill-down capability to review all levels of the hierarchy.
3. **HCA Agent (Level 3) Dashboard -** Used to monitor risk of A/OPCs and A/BOs. This dashboard provides drill-down capability to review all A/BO and A/OPC users under their responsibility.
4. **A/OPC Dashboard -** Used to monitor risk of A/BOs. This dashboard provides drill-down capability to review A/BO users under their responsibility. The A/OPC Supervisor has the same Dashboard view as the A/OPC with all the same information.
5. **A/BO Dashboard -** Used to monitor risk of cardholders who report directly to the A/BO. This dashboard provides drill-down capability to review the data of all cardholders under their responsibility. The A/BO Supervisor has the same Dashboard view as the A/BO with all the same information.

Note: Only the Navy users have a High-Level A/OPC Dashboard for the High-Level A/OPCs.

Elements of the Dashboard

Dashboards assess risk for each individual control based on specific thresholds. Also, based on the risk assessment of each of the twelve controls, an overall risk assessment is calculated for the user's hierarchical level. The drill-down capability in each control allows users to see more detail and understand the data that supports the exceptions and the risk assessment.

The RA Application assesses risk as either:

= Low (green)

= Medium (yellow)

= High (red)

At the A/BO hierarchy level, risk is assessed as either low or high for each control. At the A/OPC hierarchy level and higher, risk is assessed as low, medium, or high for each control. The overall risk assessment is designated as low, medium, or high for all dashboards.

There are a number of general elements (Figure 13) that appear on the dashboards and display information to the users:

DRAFT

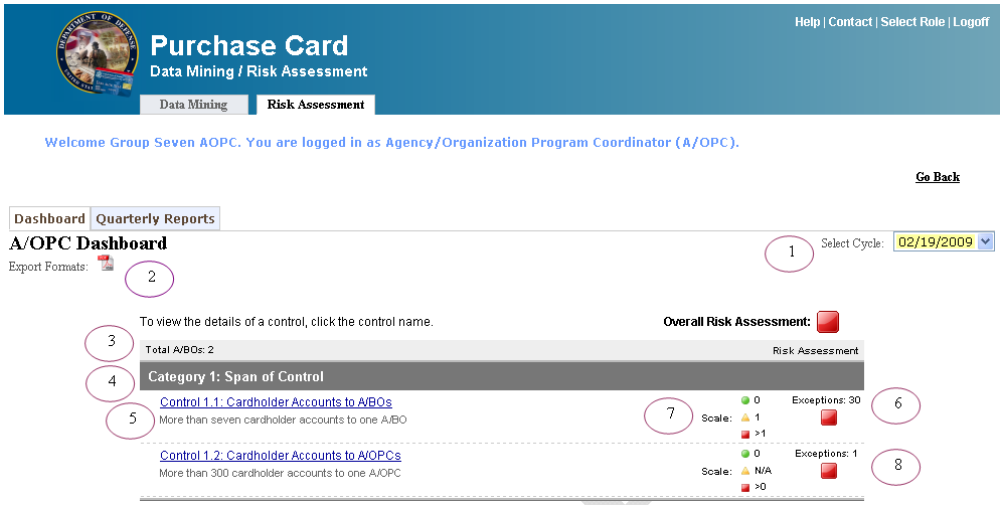


Figure 13: Dashboard Elements

1. **Select Cycle** - The Select Cycle element is a drop-down list that allows users to select the billing cycle data displayed on the dashboard. It provides a list of up to 18 billing cycles to choose from. Selecting a new billing cycle will automatically refresh the dashboard with that cycle's data. The currently selected cycle is always highlighted in yellow. The Select Cycle element applies to the entire dashboard.
2. **Export Formats** - The Export Formats element displays icons of the file format a user can export the dashboard to, allowing the user to view the dashboard outside of the web-browser. Clicking on the icon of the desired format will automatically export the dashboard in that format. Dashboards can only be exported to the PDF format. The Export Formats element applies to the entire dashboard.
3. **Hierarchy Level Count** - The Hierarchy Level Count element displays the number of users in the hierarchy one level below the reporting level. For example, for an Acquisition Executive Agent (Level 2), it will display all the HCA Agents (Level 3) under their responsibility. For an A/BO, it will display all the cardholders under the A/BO's purview. The Hierarchy Level Count element applies to the entire dashboard.
4. **Category Label** - The Category Label element displays the same categories listed in Figure 12. They segment the controls listed on the dashboard into groups of similar controls. The Category Label element applies to groups of controls.
5. **Control Title and Description** - The Control Title and Description element identifies and describes each control on the dashboard. are specific to individual controls.
6. **Exception Count** - The Exception Count element is only available on the A/OPC and A/BO dashboards. It displays the number of exceptions identified for a control. For example, for Control 4.2: Account Usage, any cardholder under an A/BO who has not used his/her card in

DRAFT

the past six billing cycles will be identified as an exception. The Exception Count element is specific to individual controls.

7. **Control Risk Assessment Exception Scale -** The Control Risk Assessment Exception scale element is available only on A/OPC dashboards. It contains ranges or numbers used to determine the risk assessment for a control based on where the Exception Count falls when compared to the scale. The ranges or numbers correspond to low-risk, medium-risk, and high-risk. The Control Risk Assessment Exception Scale element is specific to individual controls.
8. **Control Risk Assessment -** The Control Risk Assessment element indicates the risk assessment for a control. A control can be assessed as low risk, medium risk, or high risk, except for the A/BO dashboard where a control can only be assessed as either low risk or high risk. Depending on the dashboard, the Control Risk Assessment will be determined by comparing the Exception Count to the Control Risk Assessment Exception Scale. The Control Risk Assessment element is specific to individual controls.
9. **Overall Risk Assessment -** The Overall Risk Assessment element indicates the assessed risk for the user's hierarchy level as low risk, medium risk, or high risk and is based on the cumulative risk assessment of each individual control. The Overall Risk Assessment element applies to the entire dashboard.

The following sections describe each dashboard of the RA Application. The details described for each dashboard include:

- Controls that are available, and
- Risk assessment scale for each control.

PCPMO Dashboard

The PCPMO Dashboard (Figure 14) allows the PCPMO representatives to assess the overall "health" of the DoD Purchase Card Program by presenting a side-by-side comparison of the risk assessments for Army, Navy, Air Force, and Other Defense Agencies. For each Service/Organization, the PCPMO Dashboard provides risk assessment for each of the twelve controls as well as an overall risk assessment. This dashboard is a combination of the Acquisition Executive Agent (Level 2) dashboards for each Service/Organization. The PCPMO users can drill-down to lower level control details.

DRAFT

Control	Army				Navy				Air Force				ODA			
Overall Risk Assessment																
Category 1: Span of Control	Level 3 Risks			Control Risk	Level 3 Risks			Control Risk	Level 3 Risks			Control Risk	Level 3 Risks			Control Risk
Control 1.1: Cardholder Accounts to A/BOs More than seven cardholder accounts to one A/BO	1	8	24		17	3	0		1	1	11		5	6	13	
Control 1.2: Cardholder Accounts to A/OPCs More than 300 cardholder accounts to one A/OPC	26	5	2		20	0	0		2	3	8		17	3	4	
Category 2: Separation of Duties																
Control 2.1: Inadequate Separation of Duties Accounts for which the cardholder and A/BO are the same individual	33	0	0		20	0	0		13	0	0		24	0	0	
Category 3: Authorization Controls																
Control 3.1: Spending Ratio - Underutilized Credit Limits Accounts for which the six cycle spend average is less than 70% of the average cycle credit limit	2	8	23		3	6	11		0	1	12		5	8	11	
Control 3.2: Single Merchant Spending Accounts that have at least ten transactions and an 80% or greater spending percentage at one merchant	33	0	0		20	0	0		13	0	0		24	0	0	
Category 4: Card Status																
Control 4.1: Delinquent Accounts Managing Accounts delinquent for 30+ days	33	0	0		9	10	1		13	0	0		24	0	0	
Control 4.2: Account Usage Accounts that have been inactive for six cycles or have never been used (Excludes newly issued cards)	2	7	24		7	7	6		0	0	13		4	4	16	
Control 4.3: Lost/Stolen Cards Accounts that have greater than one lost/stolen card(s) in the last 12 cycles	33	0	0		20	0	0		13	0	0		24	0	0	
Category 5: Transaction Review Controls																
Control 5.1: Average Cycle Transactions Reviewed Higher than average number of transactions (>100) per cycle reviewed by the A/BO, based on three cycles of data	33	0	0		20	0	0		13	0	0		24	0	0	
Control 5.2: A/BO Response Rate A/BO failure to initiate case review in Case Management for flagged transactions within ten days	33	0	0		20	0	0		13	0	0		24	0	0	
Control 5.3: Flagged Transaction Determination Flagged transactions determined to be other than valid in Case Management (Misuse/Abuse/Suspected Fraud)	33	0	0		20	0	0		13	0	0		24	0	0	
Control 5.4: Convenience Check Amounts Convenience Checks over $3,000	33	0	0		20	0	0		13	0	0		24	0	0	

Figure14: PCPMO Dashboard

1. The example in Figure 14 shows the overall risk assessment for each Service/Organization represented by the red squares and yellow triangle on the dashboard.
2. Also it shows the risk assessment for each Service/Organization's controls. For example, Control 1.1 Cardholders to A/BOs, shows the risk assessment for Navy as low and Army, Air Force, and Other Defense Agencies as high.

To view the control report for Control 1.1, see Figure 46 in Section 6.6 (page 71).

Acquisition Executive Agent (Level 2) Dashboard

The Acquisition Executive Agent (Level 2) Dashboard (Figure 15) assesses the risk of the Service/Organization (Army, Air Force, Navy, and Other Defense Agencies). This dashboard assesses risk for the Acquisition Executive Agent (Level 2) based on the cumulative risk of all the HCA Agents (Level 3) under the purview of the Acquisition Executive Agent (Level 2) for that Service/Organization. For example in Figure 15, Control 1.1 risk assessment is assessed as high because of the 33 HCA Agents (Level 3) under the purview of the Level 2, 24 are assessed as high, eight are assessed as medium, and one is assessed as low. The dashboard provides a risk assessment for each control as well as an overall risk assessment for the level. The Acquisition Executive Agent (Level 2) can drill-down to each of the lower review levels (HCA Agent (Level 3), High-Level A/OPC, A/OPC, and A/BO).

DRAFT

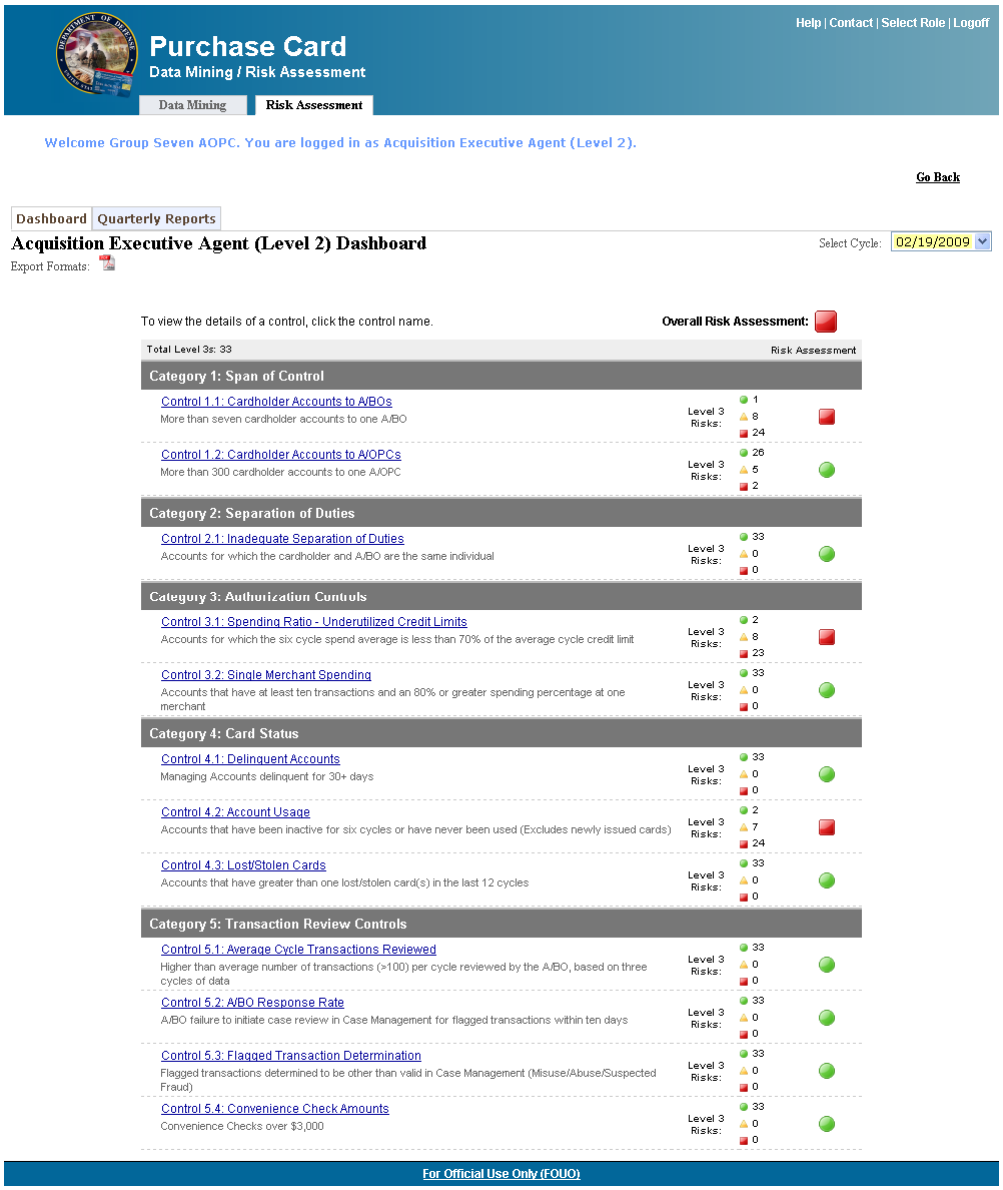


Figure 15: Acquisition Executive Agent (Level 2) Dashboard

To view the control report for Control 1.1, see Figure 47 in Section 6.6 (page 72).

HCA Agent (Level 3) Dashboard

The HCA Agent (Level 3) Dashboard (Figure 16) assesses risk for the HCA Agent (Level 3) user based on the cumulative risk of all the High-Level A/OPCs (the Navy only) and A/OPCs that fall under their hierarchy. For example in Figure 16, under Control 1.1, risk is assessed as high risk because out of the 93 A/OPC in the hierarchy, 50 are assessed as high risk, 21 are assessed as medium risk, and 22 are assessed as low risk. The dashboard provides a risk assessment for each control as well as an overall risk assessment for the level. The HCA Agent (Level 3) can drill-down on each control to see individual High-Level A/OPC (the Navy only), A/OPC, A/BO and cardholder data in the hierarchy under their purview.

DRAFT

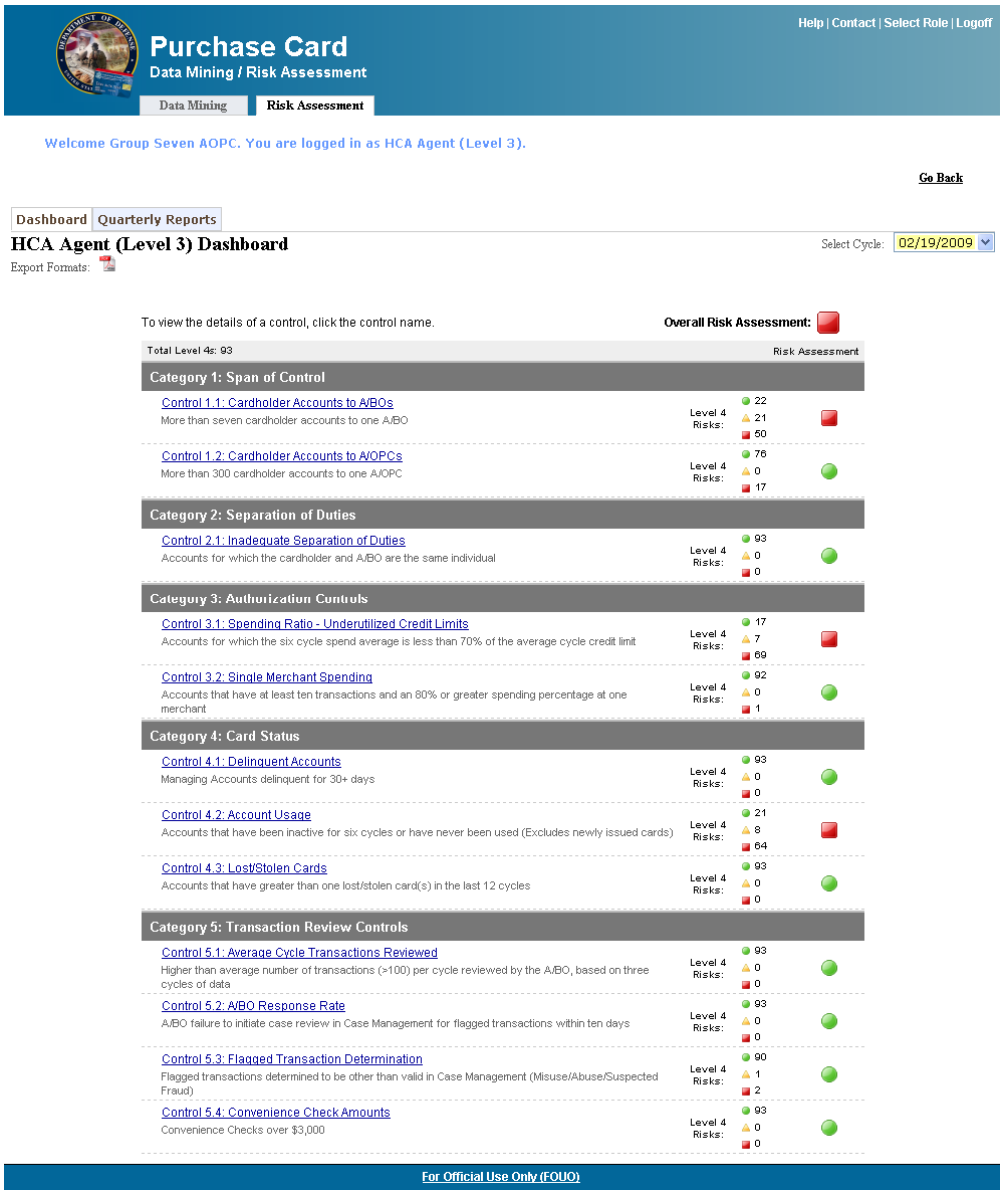


Figure 16: HCA Agent (Level 3) Dashboard

To view the control report for Control 1.1, see Figure 48 in Section 6.6 (page 73)

High-Level A/OPC Dashboard

The High-Level A/OPC Dashboard (Figure 17) assesses risk for the High-Level A/OPC user based on the cumulative risk of all the A/OPCs that fall under their hierarchy. Note: The Navy is the only Service that includes High-Level A/OPC users. For example in Figure 17, under Control 1.1, risk was assessed as low because of the seven A/OPCs in the hierarchy, one is assessed as high risk, none are assessed as medium risk, and six are assessed as low risk. The dashboard provides a risk assessment for each control as well as an overall risk assessment for the level. The High-Level A/OPC can drill-down on each control to see each individual A/OPC, A/BO and cardholder data in the hierarchy under their purview.

DRAFT

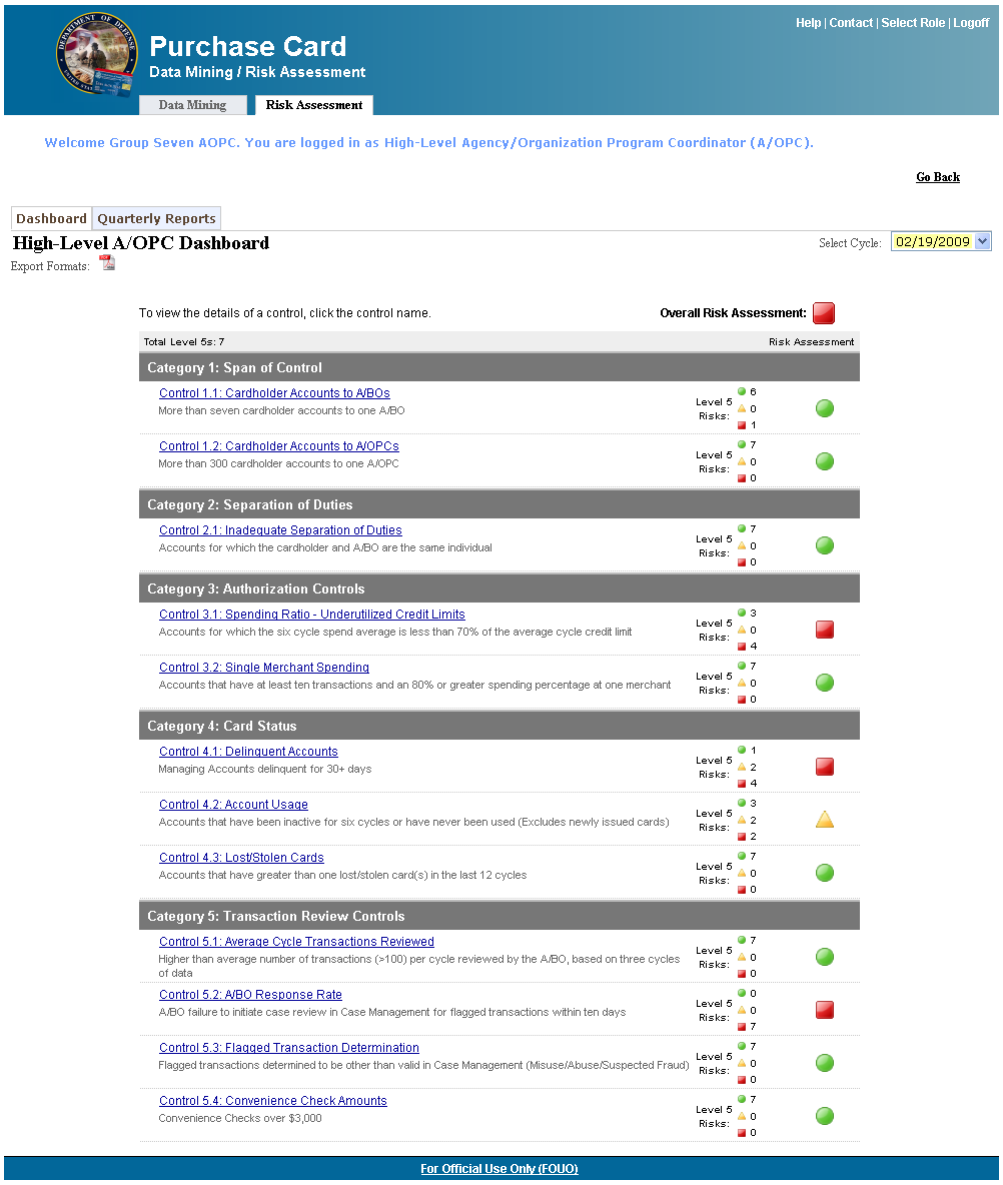


Figure 17: High-Level A/OPC Dashboard

To view the control report for Control 1.1, see Figure 49 in Section 6.6 (page 74)

A/OPC Dashboard

The A/OPC Dashboard (Figure 18) assesses risk for the A/OPC user based on the exceptions for all A/BOs under their hierarchy. For example in Figure 18, under Control 1.1, risk is assessed as high risk because the total number of exceptions of all the A/BOs reporting directly to the A/OPC is greater than one. The dashboard provides a risk assessment for each control as well as an overall risk assessment for the A/OPC. The A/OPC can drill-down on each of the controls to review A/BO and cardholder data under their purview. The A/OPC Supervisor has the same Dashboard view as the A/OPC with all the same information.

DRAFT

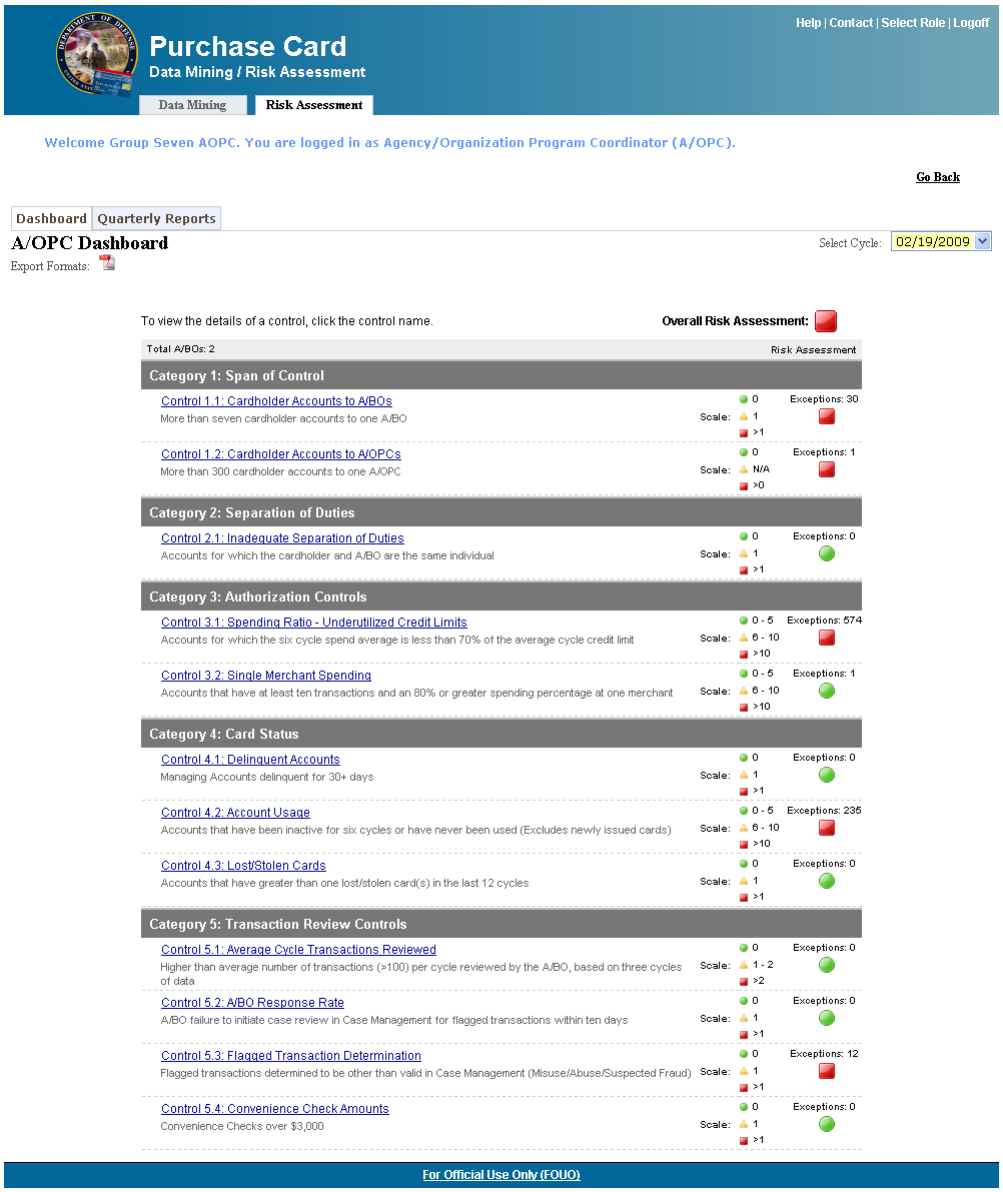


Figure 18: A/OPC Dashboard

To view the control report for Control 1.1, see Figure 50 in Section 6.6 (page 75).

A/BO Dashboard

The A/BO Dashboard (Figure 19) presents the A/BO level risk assessment. It provides a risk assessment for each control as well as an overall risk assessment for the A/BO. The A/BO Dashboard contains all the controls listed in Figure 12 (page 29) with the exception of Control 1.2 which is not relevant for A/BOs. Controls on the A/BO Dashboard can only be assessed as either low or high risk. The number of exceptions reported by a control determines the control's risk level. For example in Figure 19, under Control 1.1 the risk is assessed as low risk because out of the four cardholders under the A/BO there are no exceptions. The A/BO Supervisor has the same Dashboard view as the A/BO with all the same information.

DRAFT

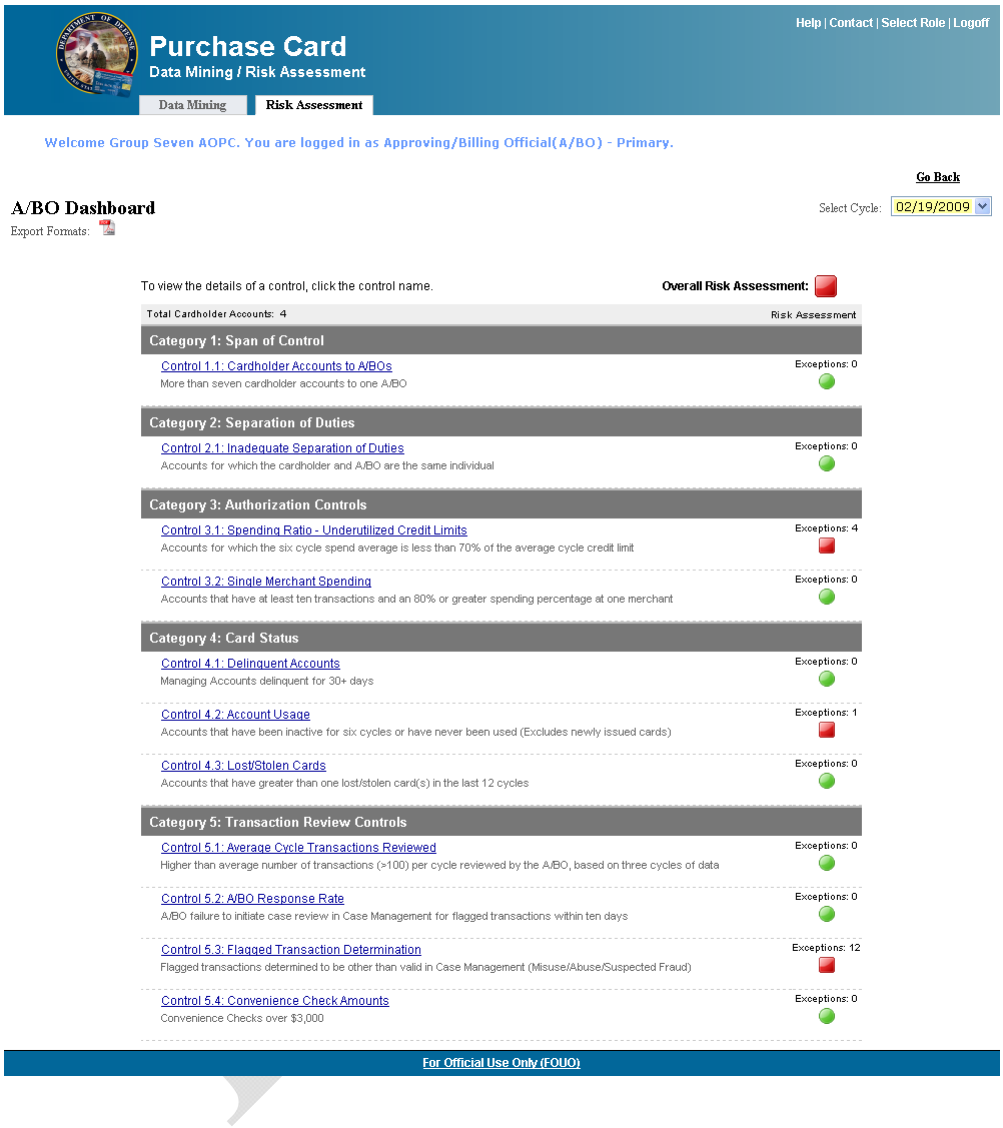


Figure 19: A/BO Dashboard

To view the control report for Control 1.1, see Figure 51 in Section 6.6 (page 76)

6.5 Viewing Control Reports

There are a number of elements that appear on the control reports that display information to the users as shown in Figure 20.1 and 20.2. They are as follows:

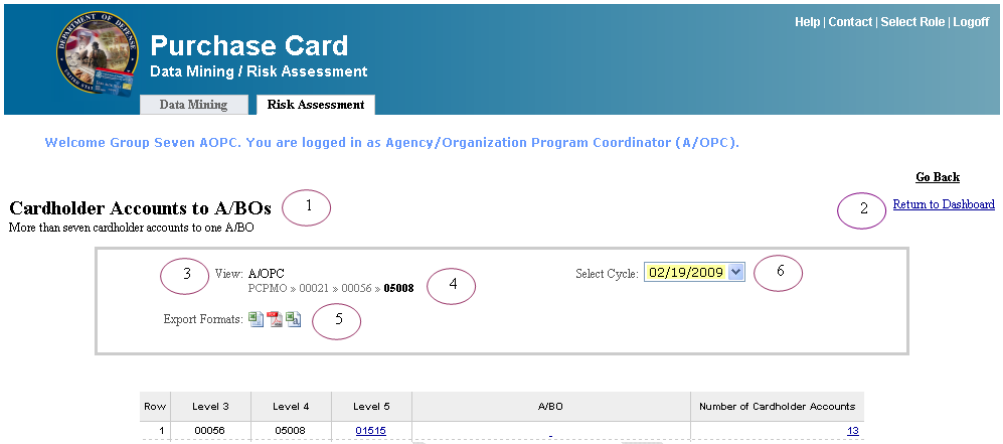


Figure 20.1: Control Elements

1. **Control Title and Description -** The Control Title and Description element identifies and describes the control.
2. **Dashboard Link -** The Dashboard Link element titled "Return to Dashboard" is a hyperlink that returns the user to his/her dashboard.
3. **Hierarchy Level Description View -** The Hierarchy Level Description View element displays the current hierarchy level description of the control report the user is viewing. The possible values for this element are PCPMO, Acquisition Executive Agent (Level 2), HCA Agent (Level 3), High-Level A/OPC, A/OPC, and A/BO.
4. **Hierarchy Level Code -** The Hierarchy Level Code element displays the current hierarchy level code of the control report the user is viewing. Users can use the Hierarchy Level Code element to navigate up the hierarchy by clicking on one of the level code hyperlinks. Users cannot navigate to a hierarchy level above their own. Any level codes that are above the user's hierarchy level are disabled.
5. **Export Formats -** The Export Formats element displays icons of the file format a user can export the dashboard to, allowing the user to view the dashboard outside of the web-browser. Clicking on an icon of the desired format will automatically export the dashboard in that format for the user. Controls can be exported to the Excel, PDF, and CSV formats.
6. **Select Cycle -** The Select Cycle element is a drop-down list that allows users to select the billing cycle they wish to view the control report for. It provides a list of up to 18 billing cycles to choose from. Selecting a new billing cycle will automatically refresh the control report with that cycle's data. The currently selected cycle is always highlighted in yellow.

DRAFT

7. **Drill-Up Icon -** The Drill-Up Icon element is a hyperlink that changes the level of detail the user is viewing by navigating the user up one level in the hierarchy (shown below in Figure 20.2). This is only available for users to navigate up to their level in the hierarchy after they have already drilled down for more detail. Users cannot drill-up above their hierarchy level.

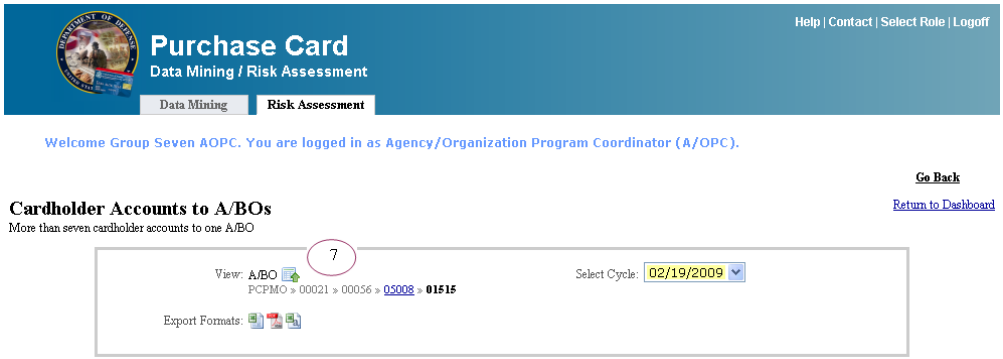


Figure 20.2: Control Elements - One Level Down

Control 1.1: Cardholder Accounts to A/BOs

Control 1.1 checks the ratio of cardholder accounts to A/BOs. The control reports as an exception all A/BOs responsible for eight or more cardholder accounts.

DRAFT

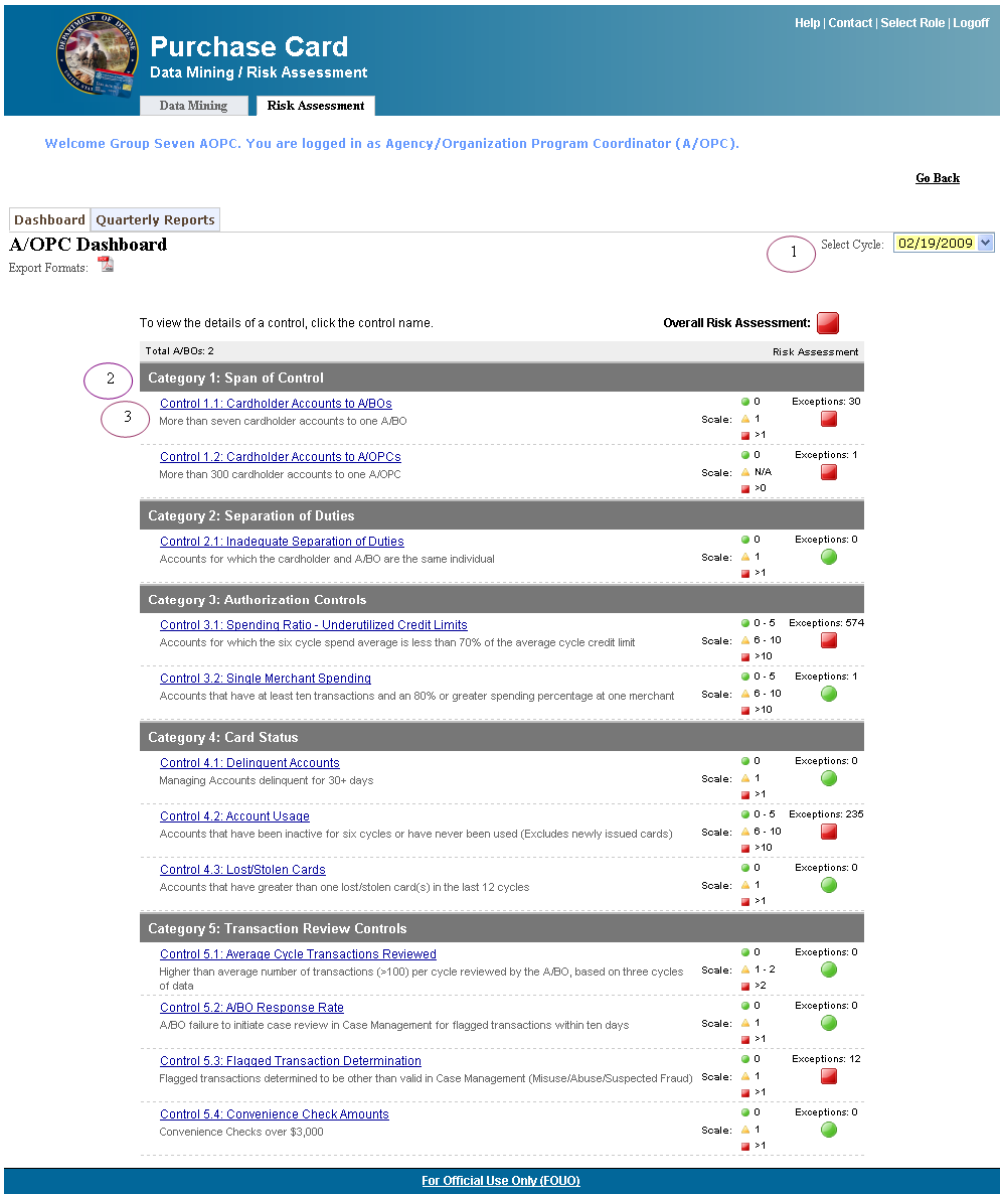


Figure 21: A/OPC Dashboard Category 1

1. Select the billing cycle from the drop-down menu to the right of the box. The billing cycle begins on the 20th of the previous month. For example, August 2010 will begin on July 20, 2010 and run through August 19th, 2010.
2. View "Category 1: Span of Control". In the example above, 30 exceptions are displayed, because under the A/OPC's responsibility the A/BOs have greater than the 7:1 ratio of cardholders to A/BOs permitted. As a result a red square indicating high risk is displayed, with the text "Exceptions: 30" above the symbol. An A/OPC dashboard risk level may appear as green (low), yellow (medium), or red (high).
3. Click the link for "Control 1.1: Cardholder Accounts to A/BOs."

An itemized list by A/BO appears (Figure 22) with the number of cardholder accounts for each A/BO displayed. The report displays the following: A/BOs and Number of Cardholder Accounts.

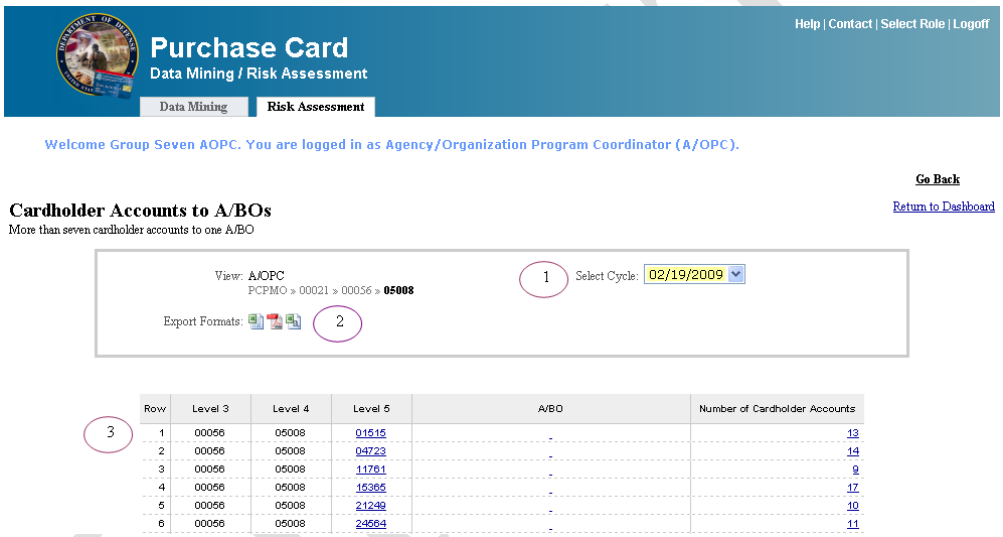


Figure 22: A/OPC Control 1.1 Detail

1. Verify the billing cycle.
2. Export the data to the preferred format: Excel, CSV, or PDF.
3. Review the exceptions reported for the control (number of cardholder accounts greater than seven)

Control 1.2: Cardholder Account to A/OPCs

Control 1.2 verifies the ratio of cardholder accounts to A/OPCs. The control will report as an exception A/OPCs responsible for more than 300 cardholder accounts.

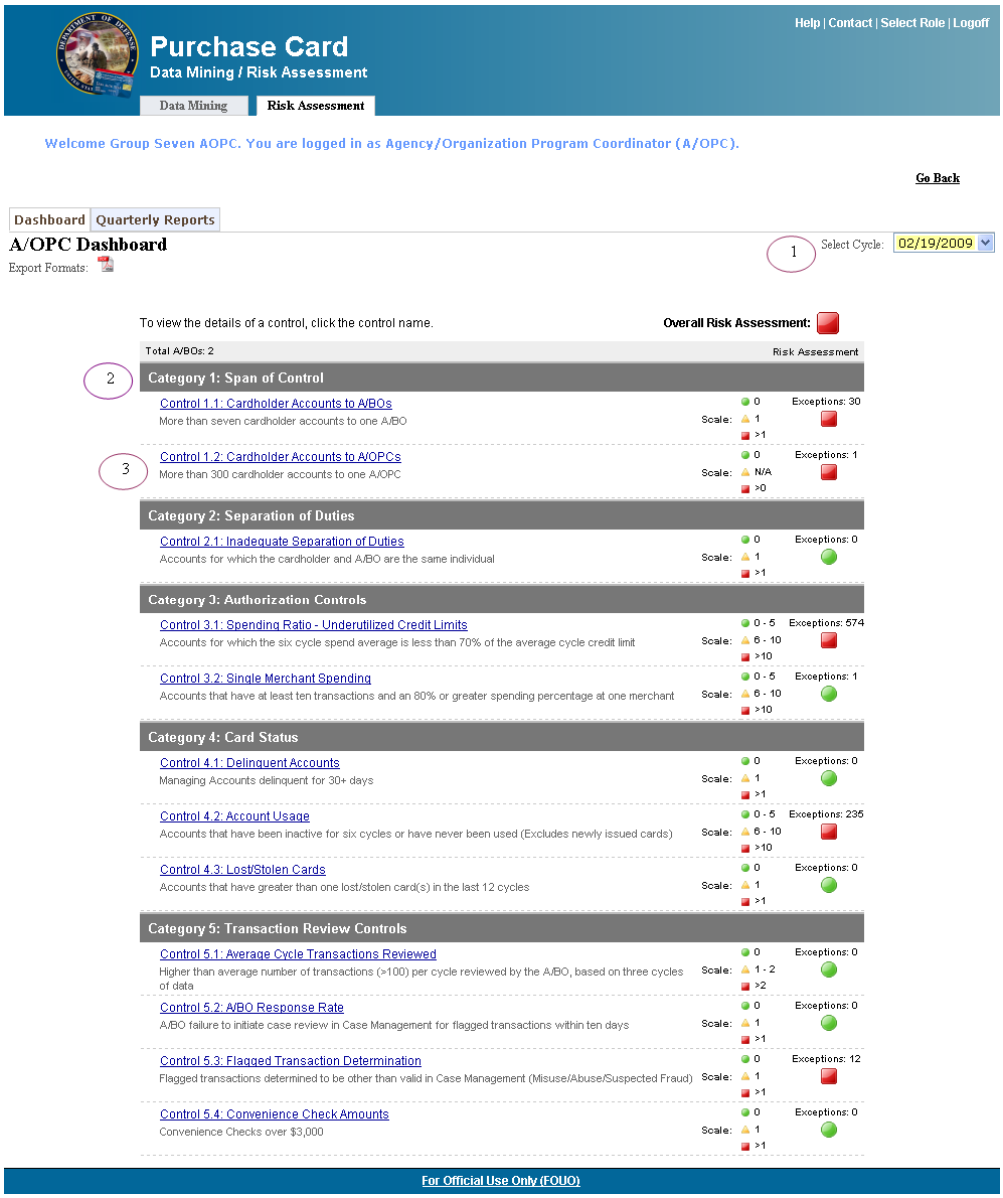


Figure 23: A/OPC Dashboard Category 1

1. Select the billing cycle from the drop-down menu to the right of the box.
2. View "Category 1: Span of Control". In the example above, a red square is displayed, indicating high risk data.

3. Click the link for "Control 1.2: Cardholder Accounts to A/OPCS."

An itemized list appears (Figure 24) with the number of cardholder accounts for each A/OPC displayed. The report displays the following: Level 4 A/OPC and Number of Cardholder Accounts.

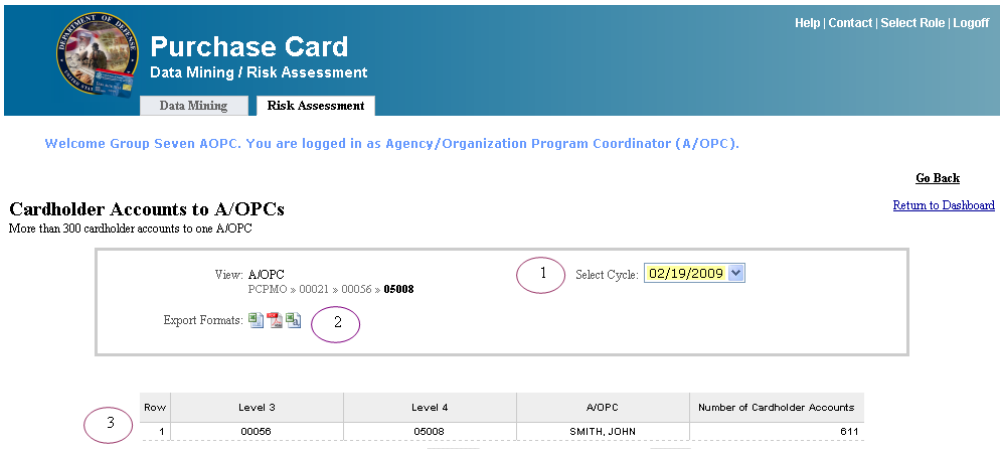


Figure 24: A/OPC Control 1.2 Detail

1. Verify the billing cycle.
2. Export the data to the preferred format: Excel, CSV, or PDF.
3. Review the exceptions reported for the control (more than 300 cardholder accounts per A/OPC).

Control 2.1: Inadequate Separation of Duties

Control 2.1 verifies separation of duties. The control will report as an exception any cardholder account where the cardholder and the A/BO are the same individual.

DRAFT

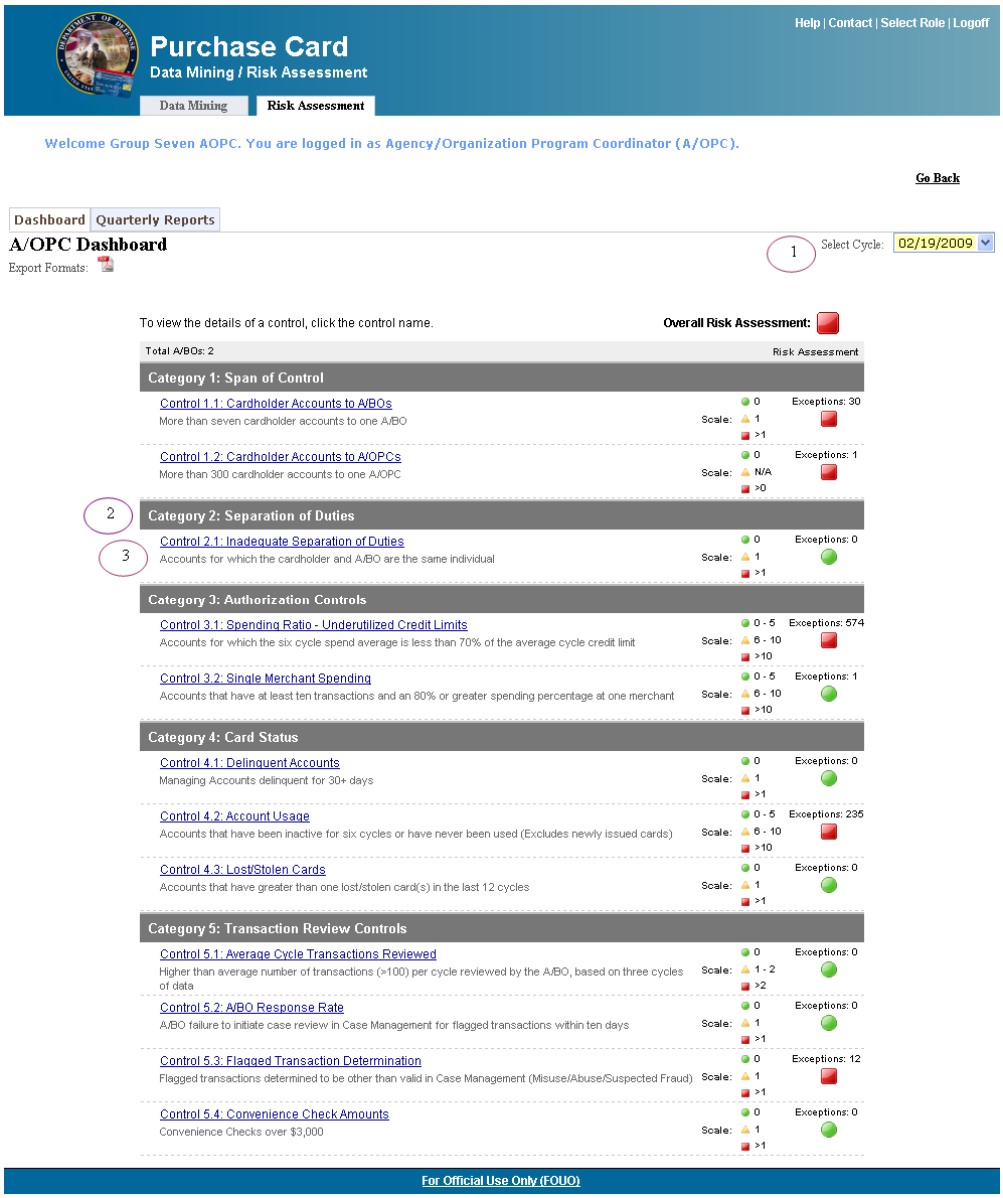


Figure 25: A/OPC Dashboard Category 2

1. Select the billing cycle from the drop-down menu to the right of the box.
2. View "Category 2: Separation of Duties". In the example above, a green circle is displayed, indicating low risk data.

3. Click the link for "Control 2.1: Inadequate Separation of Duties."

An itemized list of cardholders and A/BOs appears (Figure 26). The report displays the following: A/BO, Number of Cardholder Accounts, and Cardholder Account Number. Only the last six digits of the cardholder account number are displayed.

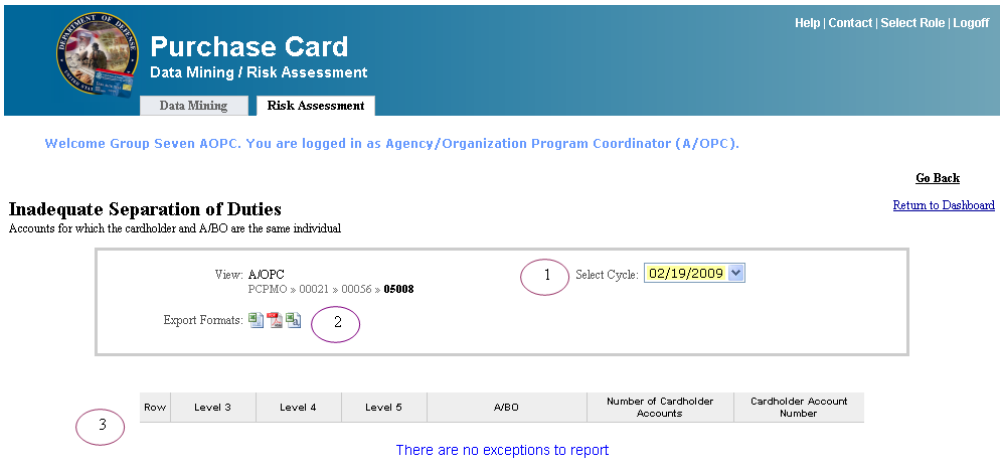


Figure 26: A/OPC Cardholders Control 2.1 Detail

1. Verify the billing cycle.
2. Export the data to the preferred format: Excel, CSV, or PDF.
3. Review the exceptions reported for the control (cardholder and A/BO are the same individual).

Control 3.1: Spending Ratio - Underutilized Credit Limits

Control 3.1 reports as an exception any cardholder accounts for which the six-cycle spend average is less than 70% of the average cycle credit limit.

DRAFT

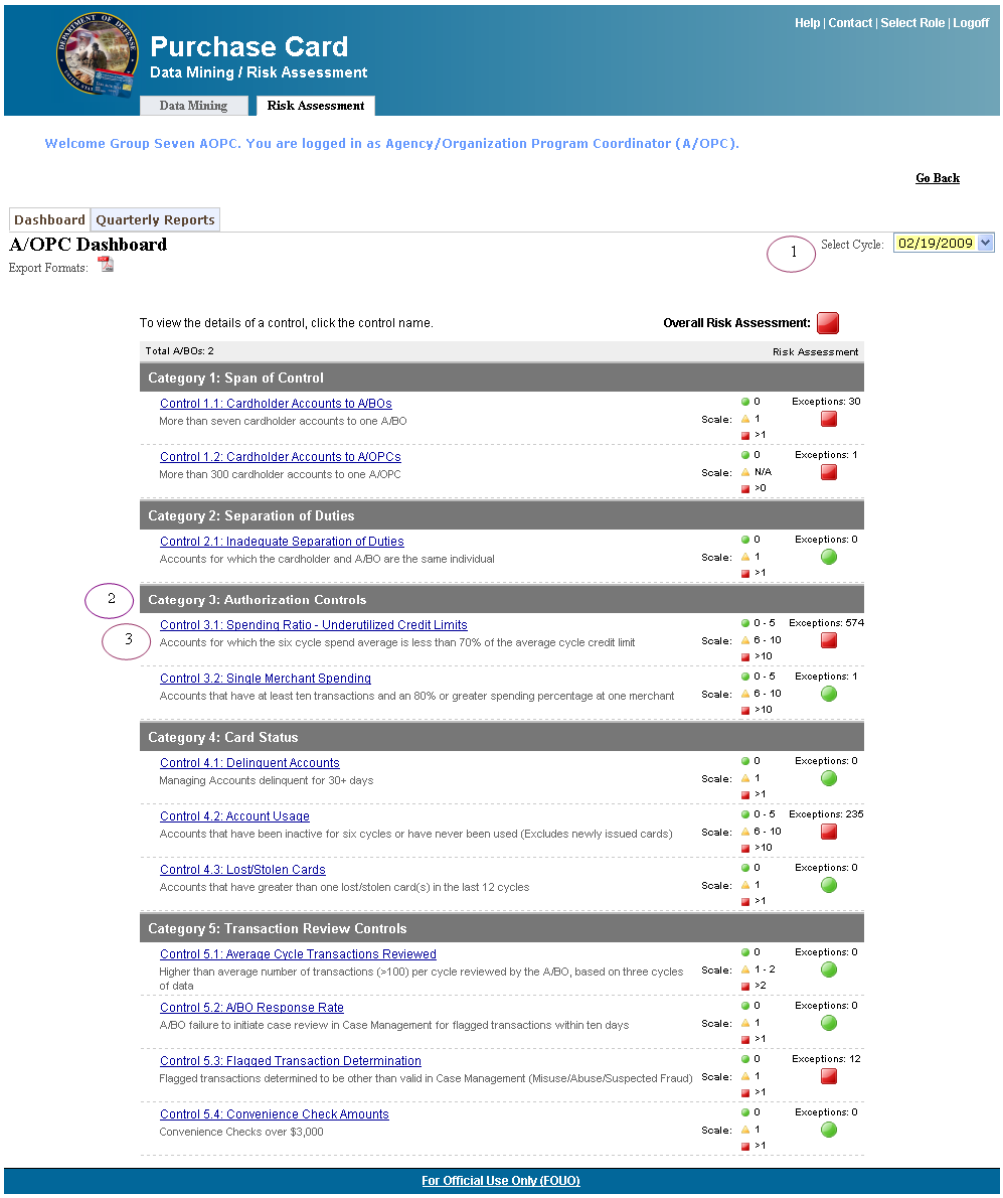
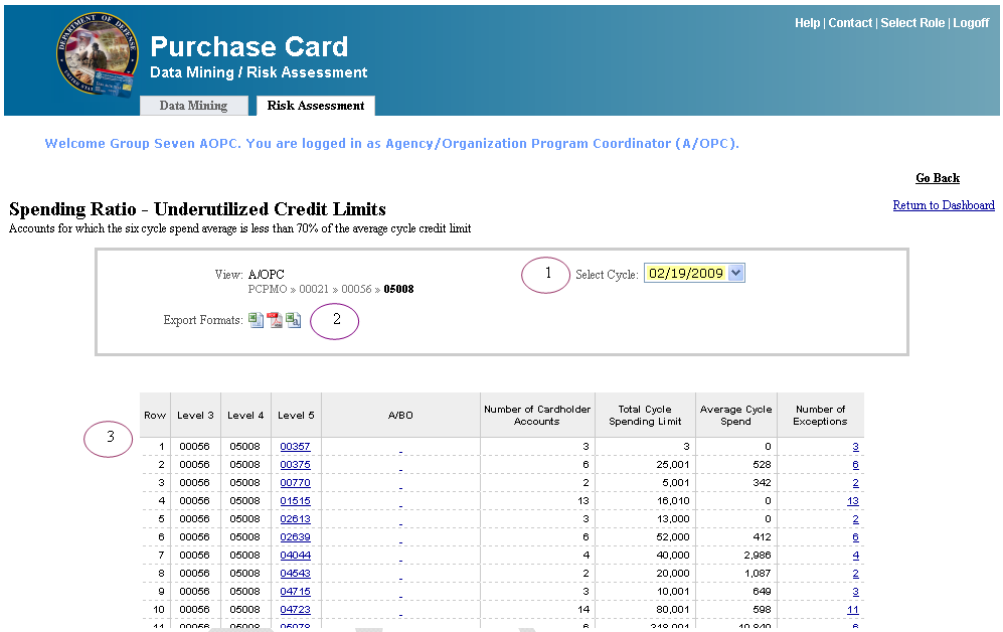


Figure 27: A/OPC Dashboard Category 3

1. Select the billing cycle from the drop-down menu to the right of the box.
2. View "Category 3: Authorization Controls." In the example above, a red square is displayed indicating high risk data.

3. Click the link for "Control 3.1: Spending Ratio - Underutilized Credit Limits."

An itemized list of A/BOs (Figure 28) for who there are underutilized credit limits appear. The report displays the following: A/BO, Number of Cardholder Accounts, Total Cycle Spending Limit, Average Cycle Spend, and Number of Exceptions.



Row	Level 3	Level 4	Level 5	A/BO	Number of Cardholder Accounts	Total Cycle Spending Limit	Average Cycle Spend	Number of Exceptions
1	00056	05008	00357	-	3	3	0	3
2	00056	05008	00375	-	6	25,001	528	6
3	00056	05008	00770	-	2	5,001	342	2
4	00056	05008	01515	-	13	16,010	0	13
5	00056	05008	02613	-	3	13,000	0	2
6	00056	05008	02639	-	6	52,000	412	6
7	00056	05008	04044	-	4	40,000	2,986	4
8	00056	05008	04543	-	2	20,000	1,087	2
9	00056	05008	04715	-	3	10,001	649	3
10	00056	05008	04723	-	14	80,001	598	11

Figure 28: A/OPC Control 3.1 Detail (rows only partially listed)

1. Verify the billing cycle.
2. Export the data to the preferred format: Excel, CSV, or PDF.
3. Review the exceptions reported for the control (cardholders whose six-cycle spend average is less than 70% of their average cycle credit limit).

Control 3.2: Single Merchant Spending

The control reports as an exception cardholder accounts that have at least ten transactions and an 80% or greater spending percentage at one merchant during the billing cycle.

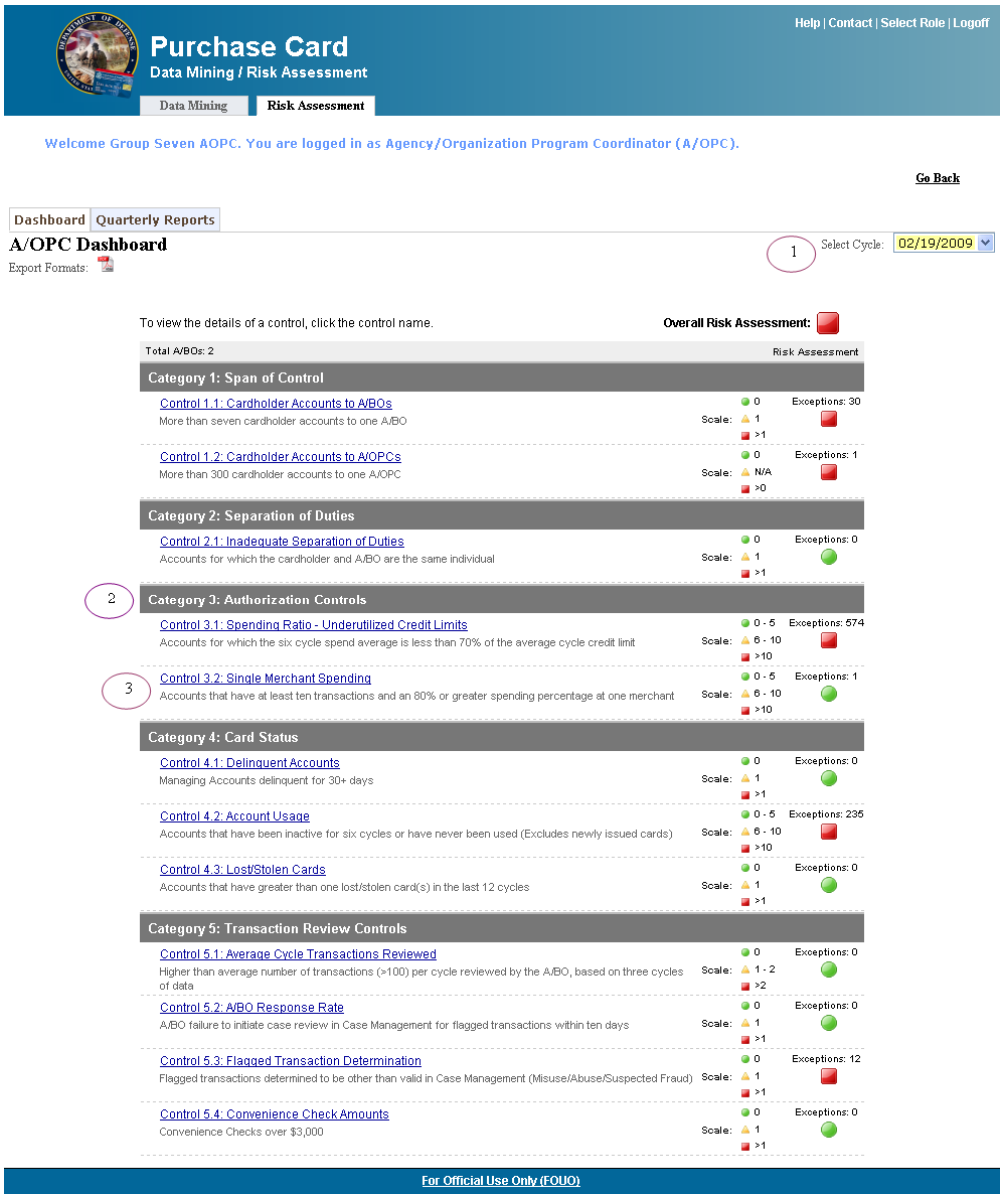


Figure 29: A/OPC Dashboard Category 3

1. Select the billing cycle from the drop-down menu to the right of the box.
2. View "Category 3: Authorization Controls." In the example above, a green circle is displayed, indicating low risk data.

3. Click the link for "Control 3.2: Single Merchant Spending"

An itemized list appears (Figure 30) with the number of cardholders for each A/BO displayed. The report displays the following: A/BO, Number of Cardholder Accounts, and Number of Exceptions.

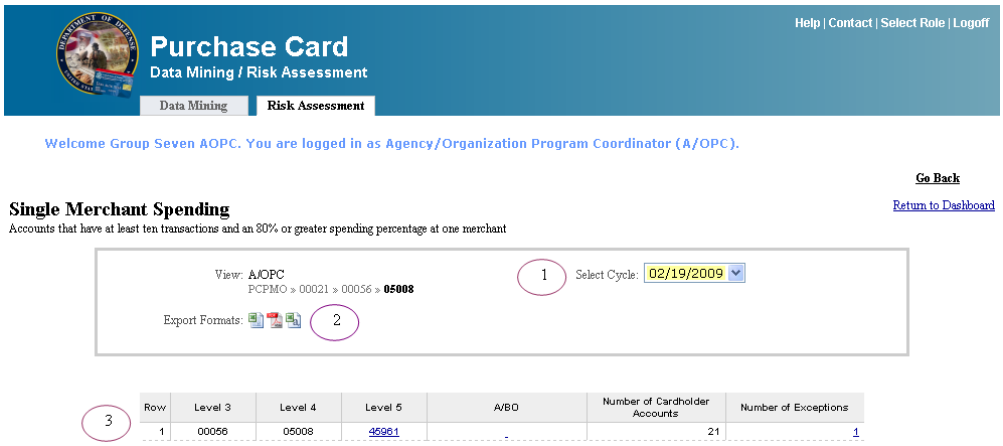


Figure 30: A/OPC Control 3.2 Detail

1. Verify the billing cycle.
2. Export the data to the preferred format: Excel, CSV, or PDF.
3. Review the exceptions reported for the control (accounts that have at least ten transactions and an 80% or greater spending percentage at one merchant).

Control 4.1: Delinquent Accounts

Control 4.1 reports as an exception managing accounts that are delinquent in payment. Managing accounts are considered delinquent if it has not been made within 30 days of the due date.

DRAFT

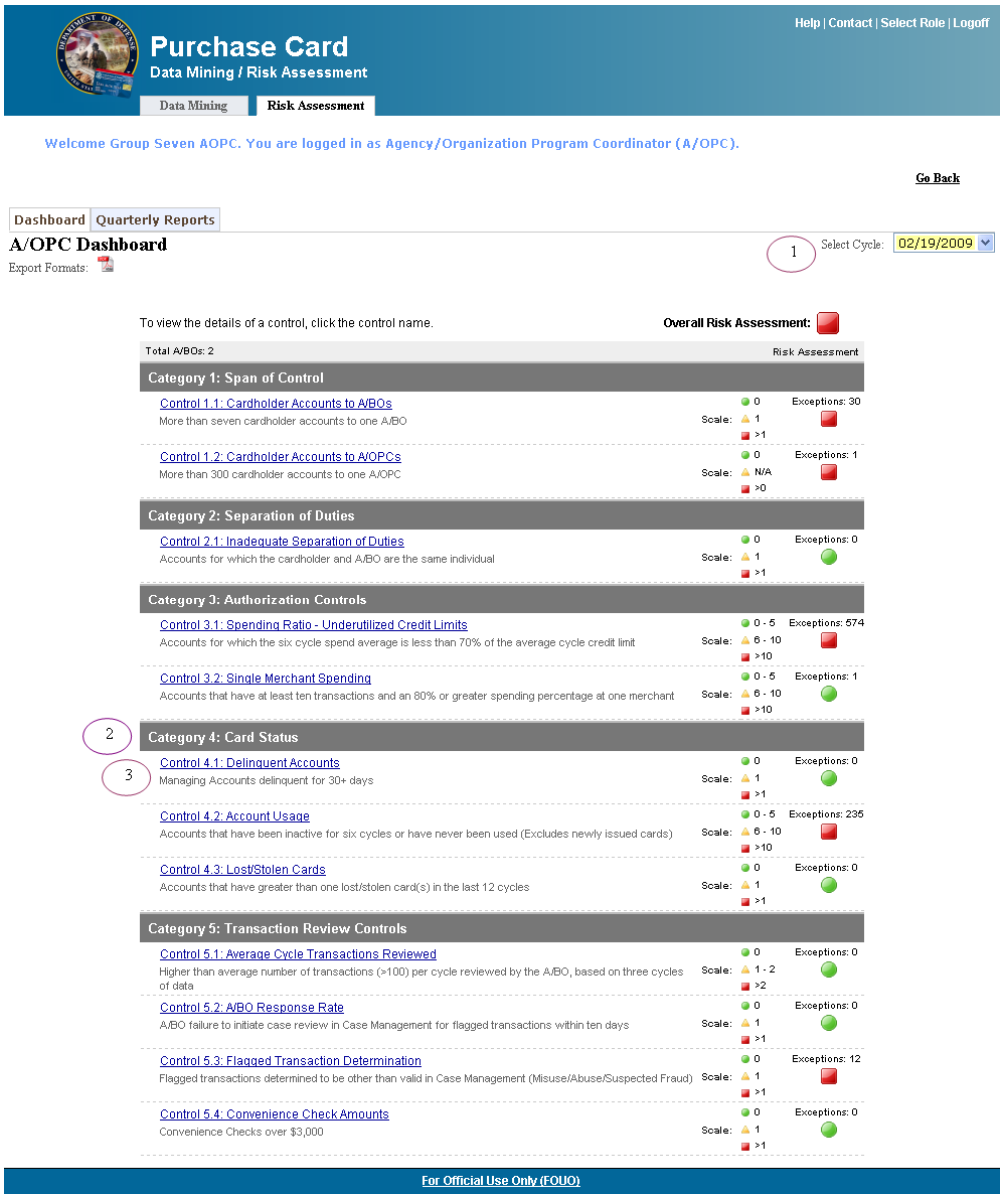


Figure 31: A/OPC Dashboard Category 4

1. Select the billing cycle from the drop-down menu to the right of the box.

2. View "Category 4: Card Status." In the example above, the green circle indicates low risk data.
3. Click the link for "Control 4.1: Delinquent Accounts."

An itemized list appears (Figure 32) for managing accounts that are 31 or more days delinquent. The report displays the following: A/BO, Number of Cardholder Accounts, Managing Account Number, Payment Posting Date, Certification Date, and Outstanding Balance.

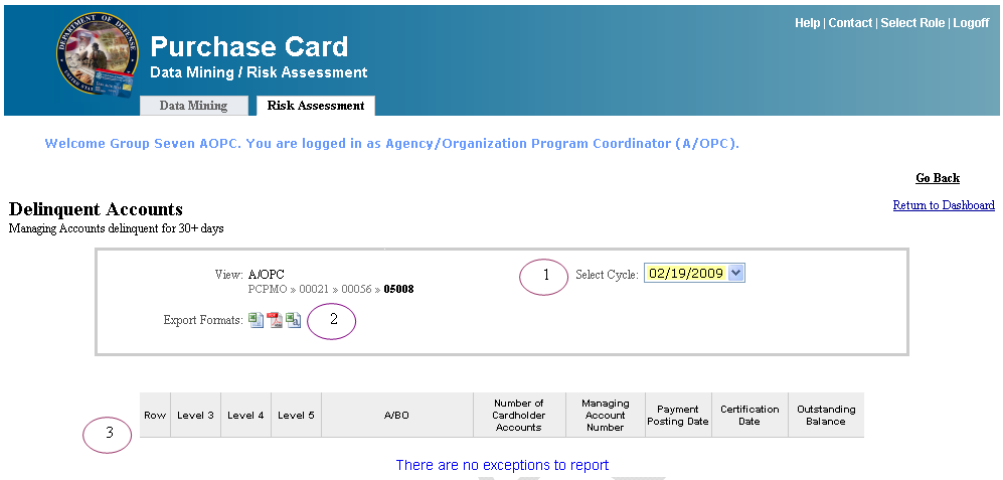


Figure 32: A/OPC Control 4.1 Detail

1. Verify the billing cycle.
2. Export the data to the preferred format: Excel, CSV, or PDF.
3. Review the exceptions reported for the control (managing accounts that are delinquent in payment for 31 days or more).

Control 4.2: Account Usage

Control 4.2 reports as an exception cardholder accounts that have been inactive for six months or have never been used. Newly issued cards less than 60 days old are excluded.

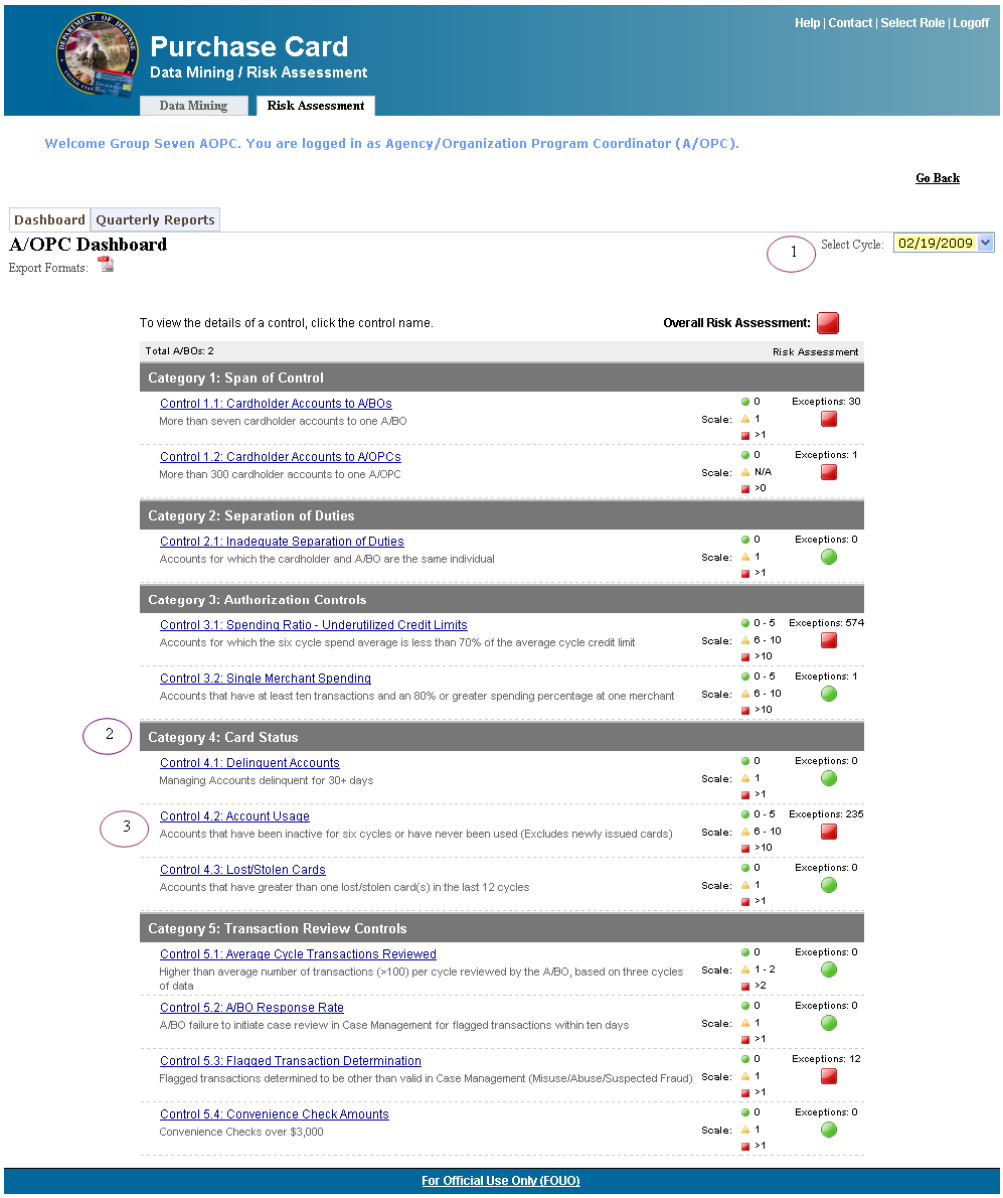
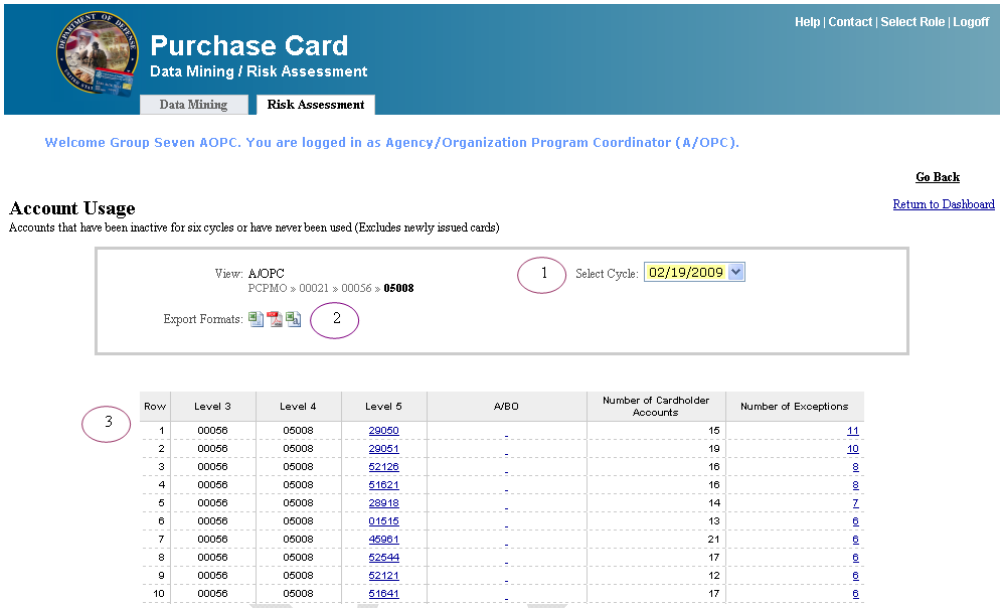


Figure 33: A/OPC Dashboard Category 4

1. Select the billing cycle from the drop-down menu to the right of the box.

2. View "Category 4: Card Status." In the example above, the red square indicates high risk data
3. Click the link for "Control 4.2: Account Usage."

An itemized list (Figure 34) appears of cardholder accounts that have been inactive for six months or more, or have not been used (excluding newly issued cards). The report displays the following: A/BO, Number of Cardholder Accounts, and Number of Exceptions.



Row	Level 3	Level 4	Level 5	A/BO	Number of Cardholder Accounts	Number of Exceptions
1	00056	05008	29050	-	15	11
2	00056	05008	29051	-	19	10
3	00056	05008	52126	-	16	8
4	00056	05008	51621	-	16	8
5	00056	05008	28918	-	14	7
6	00056	05008	01515	-	13	6
7	00056	05008	45961	-	21	6
8	00056	05008	52544	-	17	6
9	00056	05008	52121	-	12	6
10	00056	05008	51641	-	17	6

Figure 34: A/OPC Control 4.2 Detail

1. Verify the billing cycle.
2. Export the data to the preferred format: Excel, CSV, or PDF.
3. Review the exceptions reported for the control (cardholder accounts that have been inactive for six billing cycles or have never been used).

Control 4.3: Lost / Stolen Cards

Control 4.3 reports as an exception all cardholder accounts that have more than one lost or stolen card in the last 12 cycles.

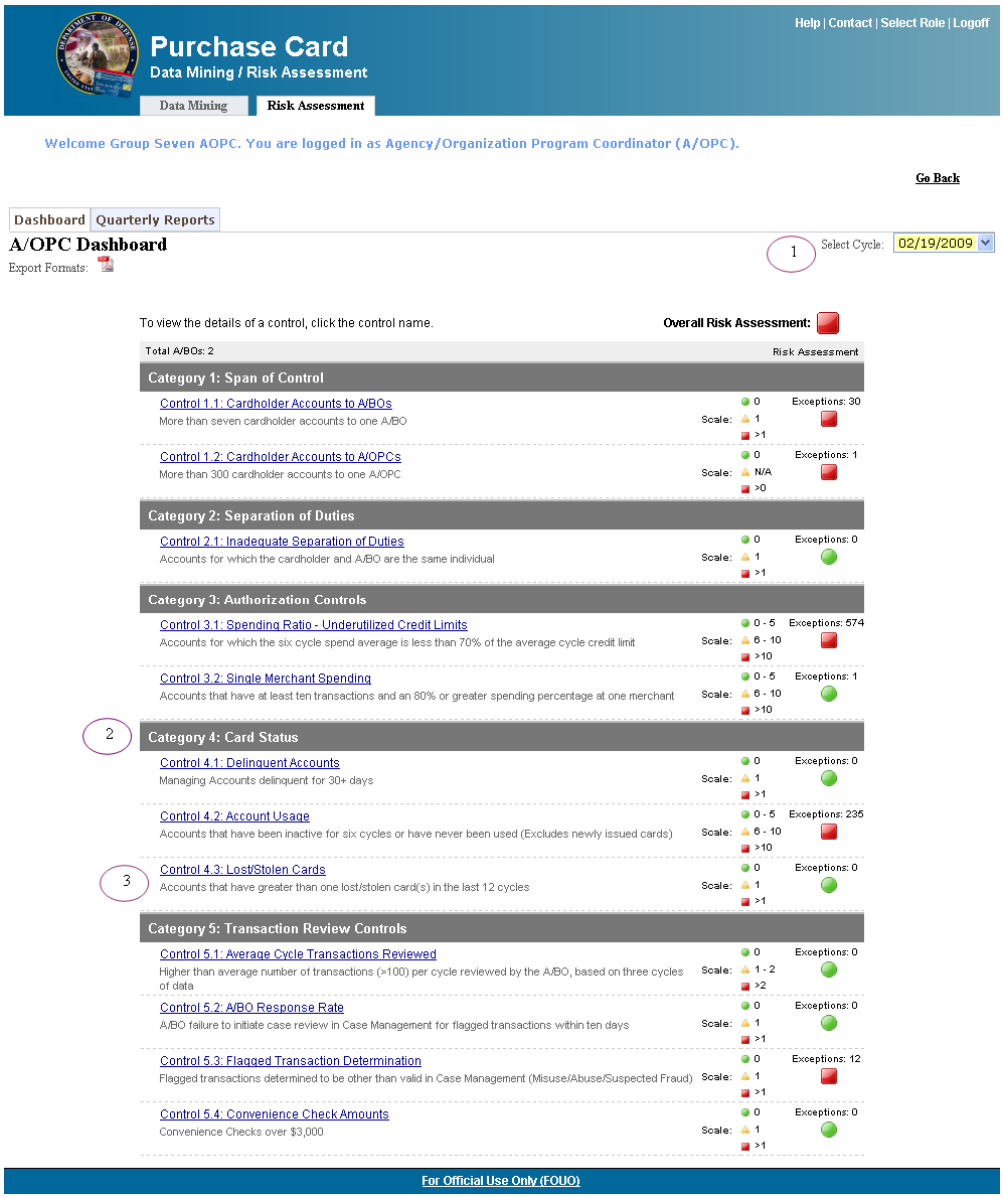


Figure 35: A/OPC Dashboard Category 4

1. Select the billing cycle from the drop-down menu to the right of the box.

2. View Category 4: Card Status." In the example above, the green circle indicates low risk data.
3. Click the "Control 4.3: Lost/Stolen Cards."

An itemized list appears (Figure 36) of cardholder accounts that have more than one lost/stolen card in the last 12 months. The report displays the following: A/BO, Number of Cardholder Accounts, and Number of Exceptions.

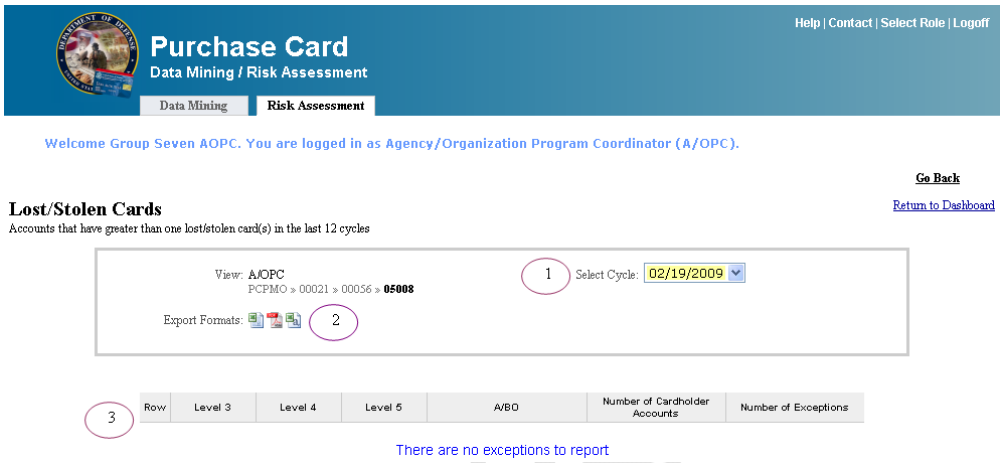


Figure 36: A/OPC Control 4.3 Detail

1. Verify the billing cycle.
2. Export the data to the preferred format: Excel, CSV, or PDF.
3. Review the exceptions reported for the control (cardholder accounts that have had greater than one lost/stolen card in the last 12 cycles).

Control 5.1: Average Cycle Transactions Reviewed

Control 5.1 reports as an exception all A/BOs who review a higher than average (greater than 100) number of transactions per billing cycle, based on the past three billing cycles of data.

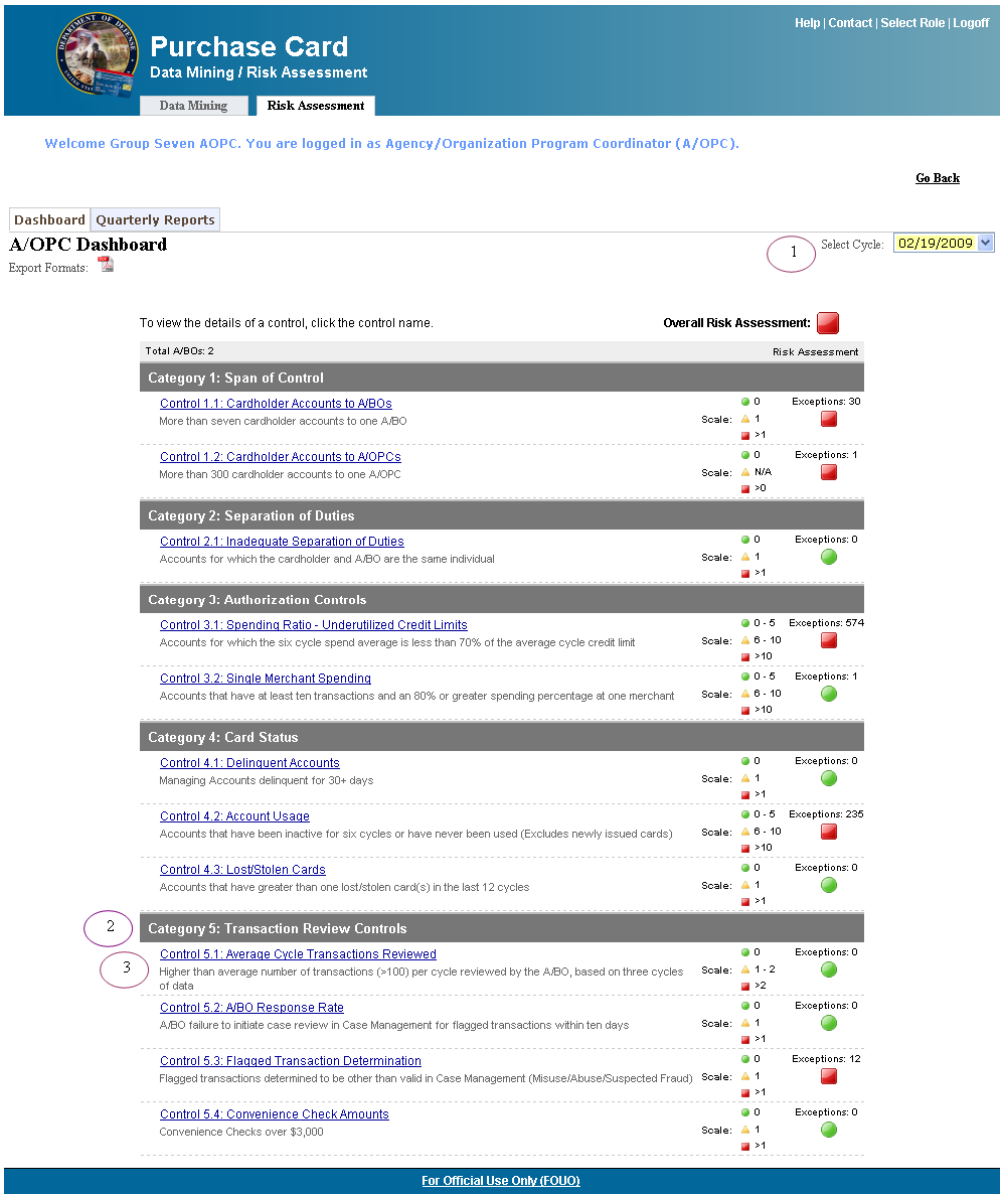


Figure 37: A/OPC Dashboard Category 5

1. Select the billing cycle from the drop-down menu to the right of the box.
2. View "Category 5: Transaction Review Controls." In the example above, the green circle indicates low risk data.

3. Click the link for "Control 5.1: Average Cycle Transactions Reviewed."

An itemized list appears (Figure 38) of cardholder accounts that have a higher than average number of billing cycle transactions reviewed per A/BO, based on three billing cycles of data. The report displays the following: A/BO, Number of Cardholder Accounts, Current Cycle Transactions, Current Cycle Spend, 3 Cycle Transaction Average, and 3 Cycle Spend Average.

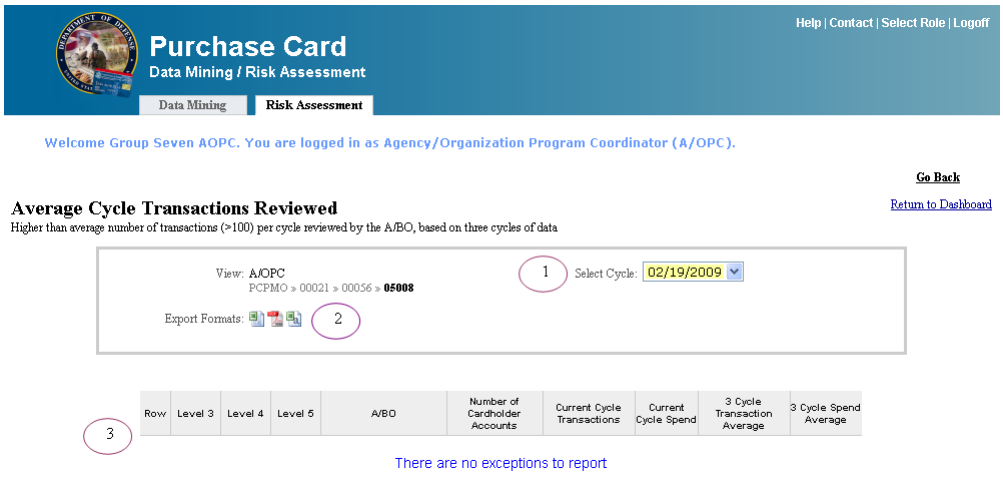


Figure 38: A/OPC Control 5.1 Detail

1. Verify the billing cycle.
2. Export the data to the preferred format: Excel, CSV, or PDF.
3. Review the exceptions reported for the control (accounts that have a higher than average number of billing cycle transactions reviewed per A/BO).

Control 5.2: A/BO Response Rate

Control 5.2 reports as an exception the number cases for which A/BOs have failed to initiate a review within 10 days of referred cases by the RA Application.

DRAFT

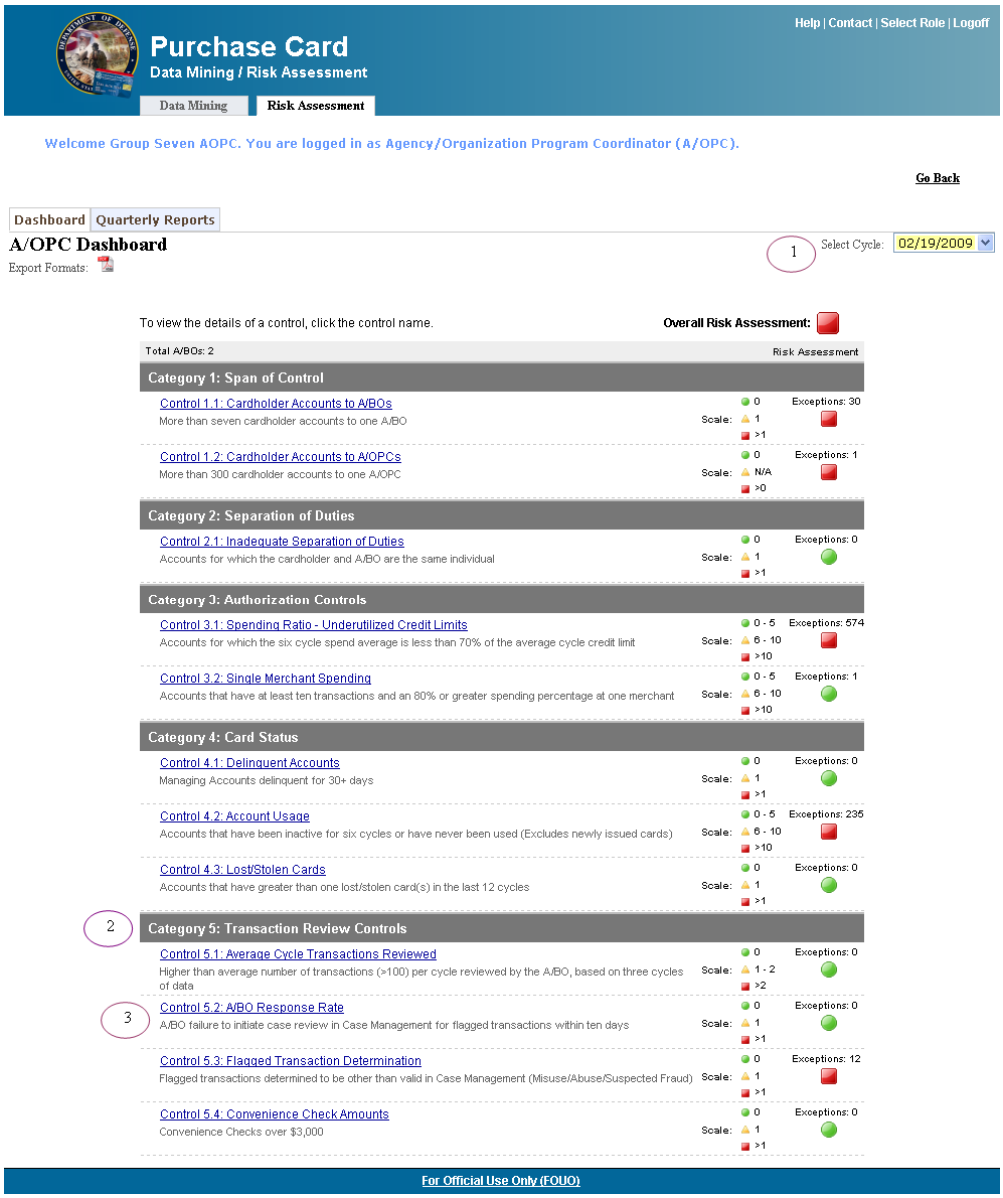


Figure 39: A/OPC Dashboard Category 5

1. Select the billing cycle from the drop-down menu to the right of the box.
2. View "Category 5: Transaction Review Controls." In the example above, the green circle indicates low risk data.

3. Click the link for "Control 5.2: A/BO Response Rate."

An itemized list appears (Figure 40) of A/BOs who did not respond to a high risk transaction notification within the 10-day limit. The report displays the following: A/BO, Number of Cardholder Accounts, Total Transactions, Flagged Transactions, Flag %, and Number of Exceptions.

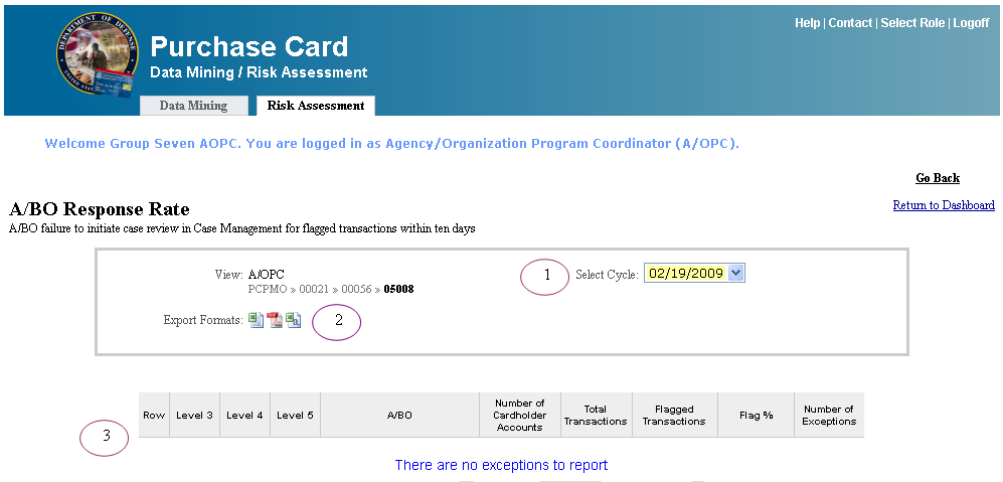


Figure 40: A/OPC Control 5.2 Detail (rows only partially listed)

1. Verify the billing cycle.
2. Export the data to the preferred format: Excel, CSV, or PDF.
3. Review the exceptions reported for the control (A/BO did not initiate a review of a referred case within the 10-day limit). The report in Figure 40 only partially shows the entire report. Users can scroll down to view all exceptions.

Control 5.3: Flagged Transaction Determination

Control 5.3 reports as an exception all flagged transactions that have been determined to be misuse, abuse, or suspected fraud.

DRAFT

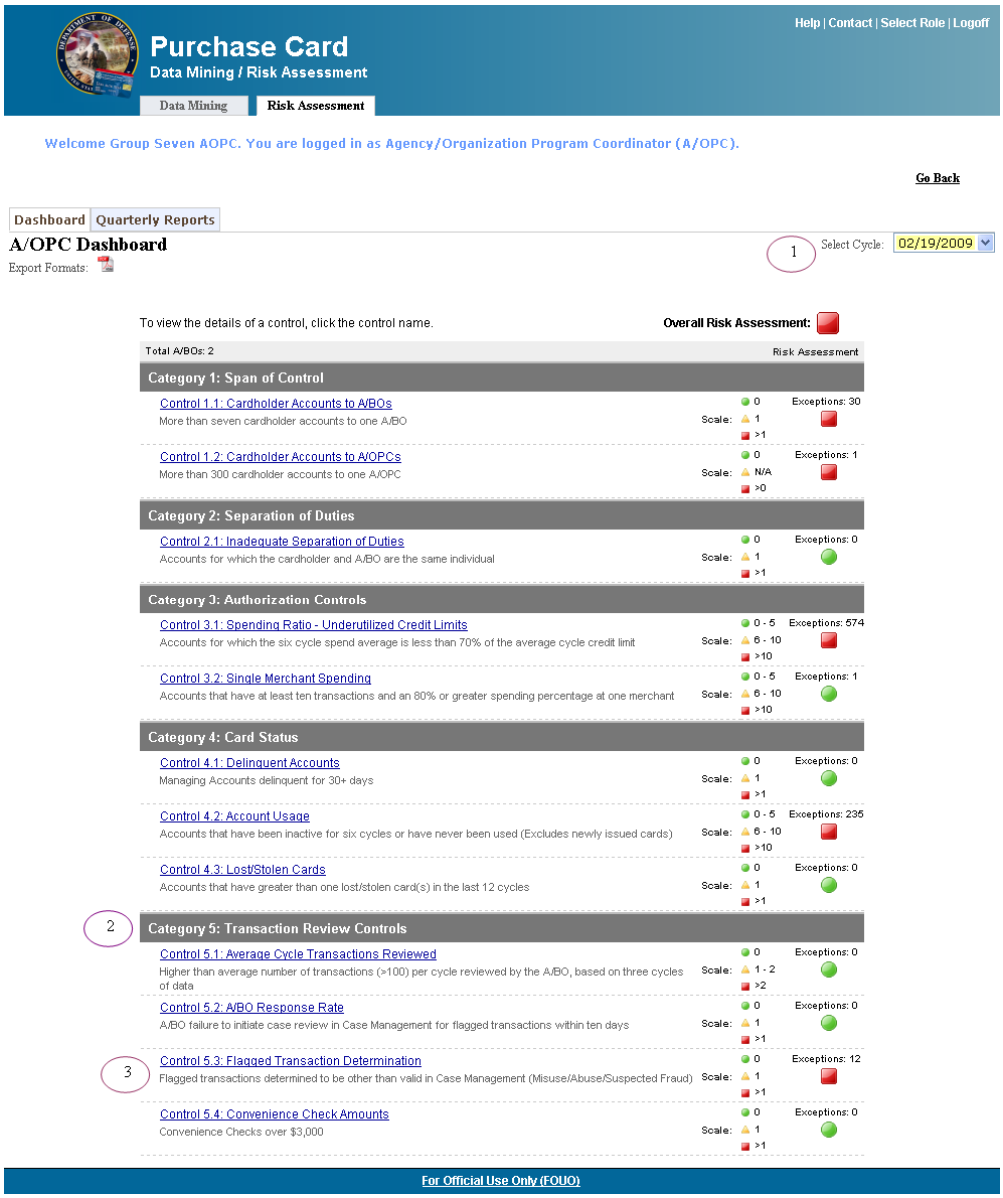


Figure 41: A/OPC Dashboard Category 5

1. Select the billing cycle from the drop-down menu to the right of the box.
2. View "Category 5: Transaction Review Controls." In the example above, the red square indicates high risk data.

3. Click the link for "Control 5.3: Flagged Transaction Determination."

An itemized list appears (Figure 42) for accounts that have flagged transactions determined not to be valid (misuse, abuse, suspected fraud). The report displays the following: A/BO, Number of Cardholder Accounts, Total Transactions, Flagged Transactions, Flag %, and Number of Exceptions.

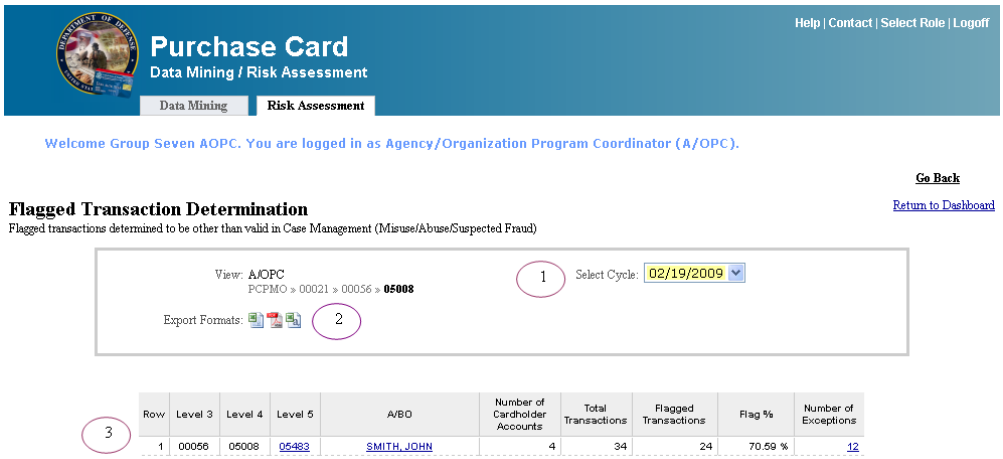


Figure 42: A/OPC Control 5.3 Detail

1. Verify the billing cycle.
2. Export the data to the preferred format: Excel, CSV, or PDF.
3. Review the exceptions reported for the control (flagged transactions that have been determined to be misuse, abuse, or suspected fraud).

Control 5.4: Convenience Check Amounts

This control reports as an exception accounts that have convenience checks over $3,000.

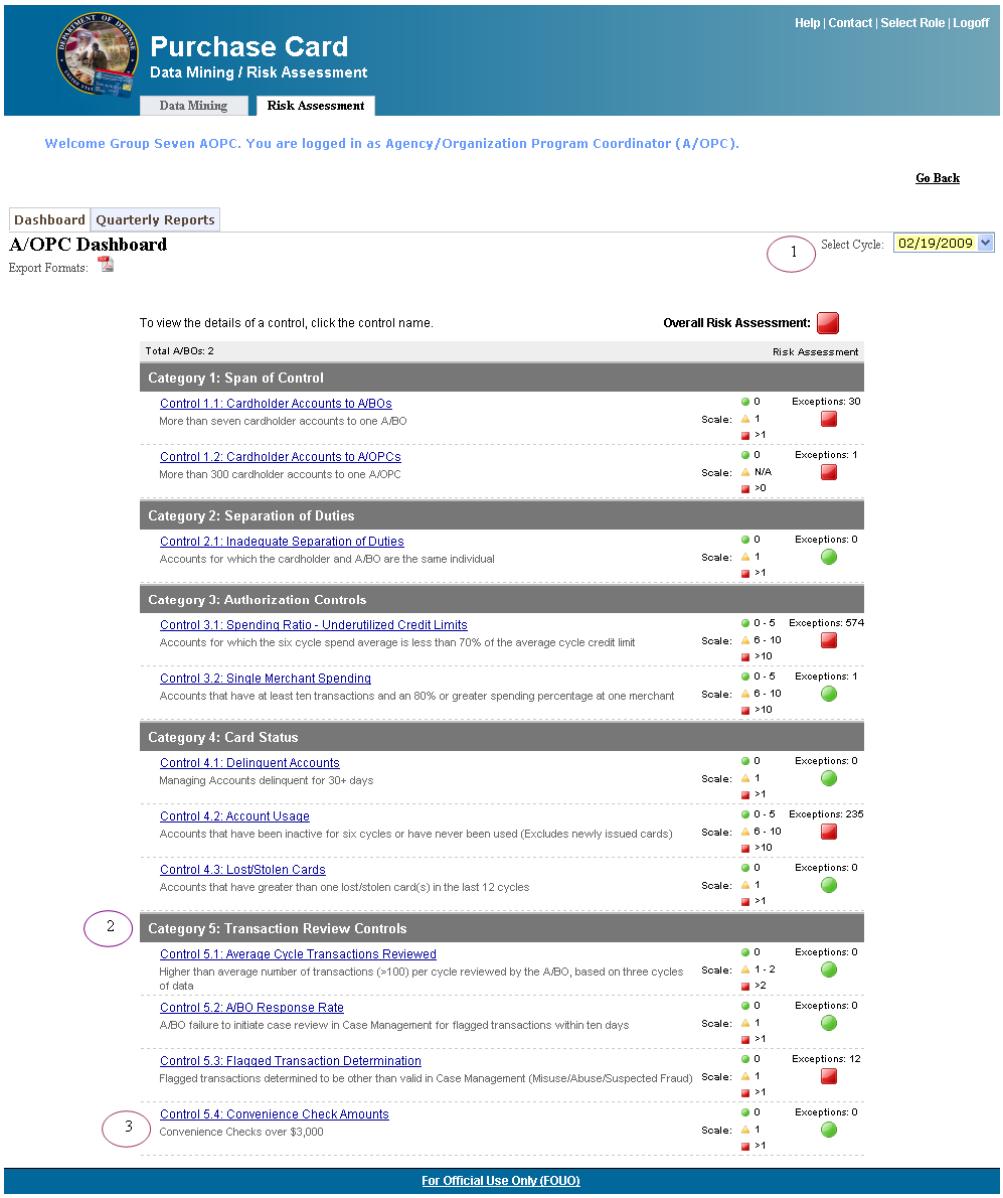


Figure 43: A/OPC Dashboard Category 5

1. Select the billing cycle from the drop-down menu to the right of the box.
2. View "Category 5: Transaction Review Controls." In the example above, the green circle indicates low risk data.

3. Click the link for "Control 5.4: Convenience Check Amounts."

An itemized list appears (Figure 44) for accounts that have convenience checks greater than $3,000. The report displays the following: A/BO, Number of Cardholder Accounts, Total Number of Checks, Dollar Value of Checks Over $3,000, and Number of Exceptions.

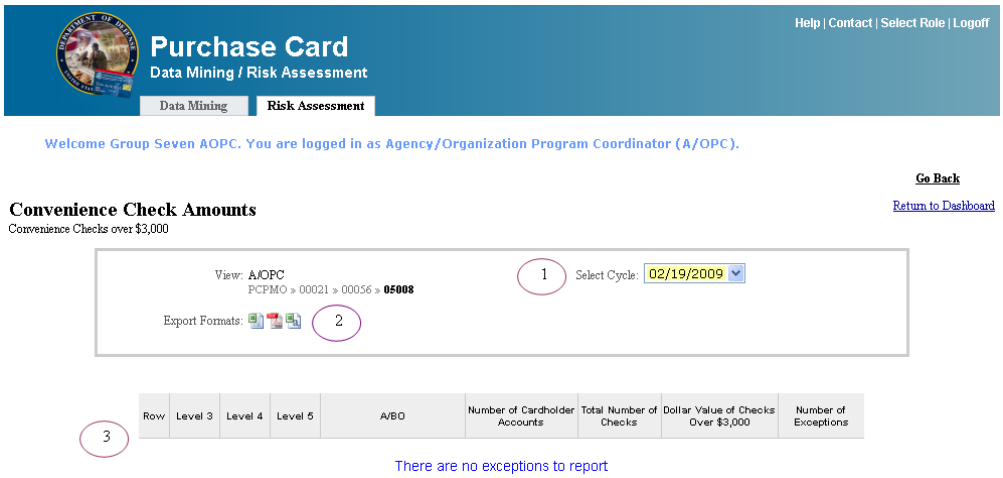


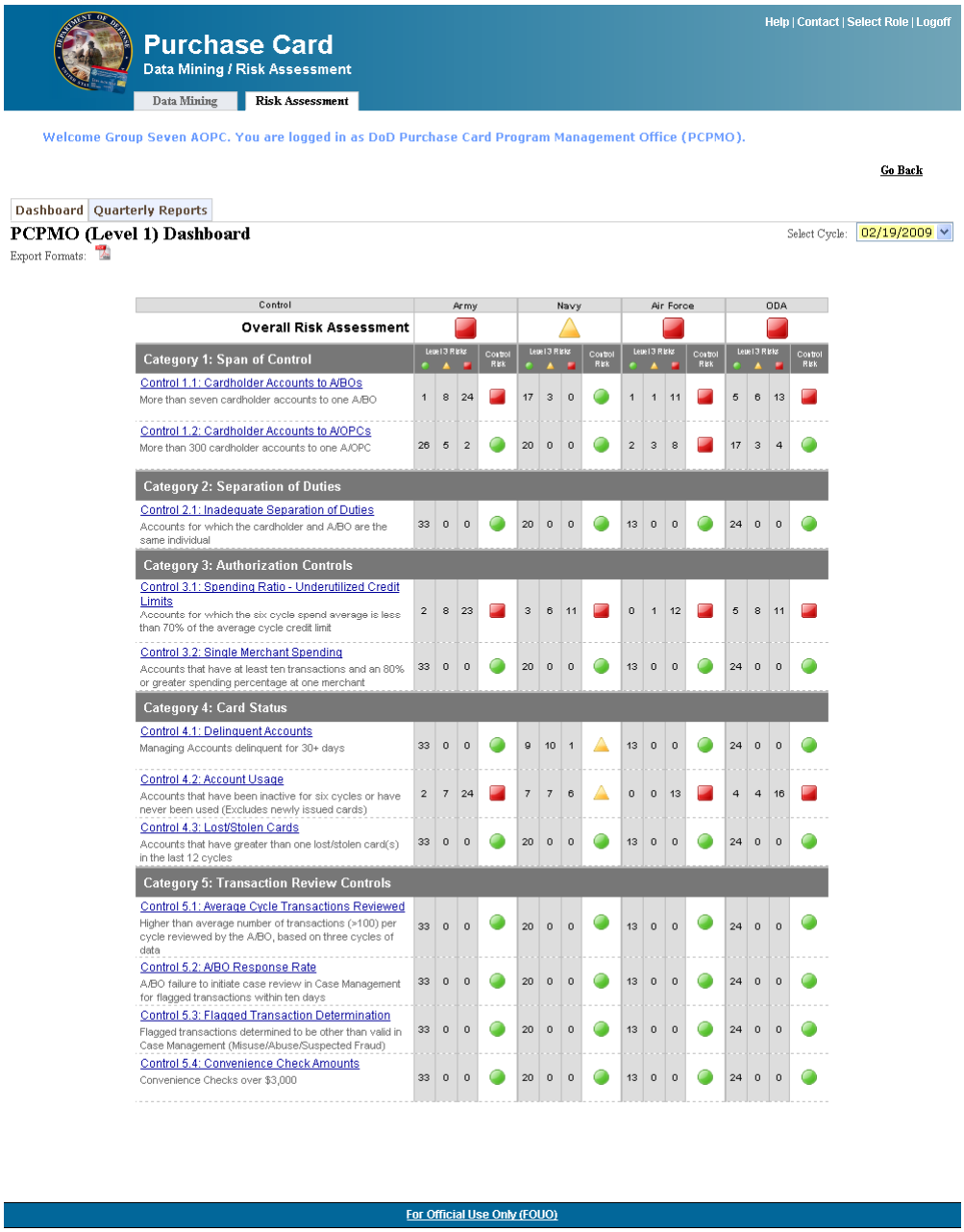
Figure 44: A/OPC Control 5.4 Detail

1. Verify the billing cycle.
2. Export the data to the preferred format: Excel, CSV, or PDF.
3. Review the exceptions reported for the control (cardholder accounts that have convenience checks greater than $3,000).

6.6 Accessing Control Reports

Control 1.1 checks the ratio of cardholder accounts to A/BOs and reports as an exception A/BOs who are responsible for eight or more cardholder accounts. Note: the example below is taken from the Navy, which has High-Level A/OPCs. All other Service/Organizations do not have High-Level A/OPCs.

As shown in Figure 45, the PCPMO dashboard control reports are accessible by clicking on the various control links within each of the five control categories. Clicking on "Control 1.1 Cardholder to A/BOs," users access the DoD PCPMO control report as shown in Figure 46.



Help | Contact | Select Role | Logoff

Purchase Card
Data Mining / Risk Assessment

Data Mining | Risk Assessment

Welcome Group Seven AOPC. You are logged in as DoD Purchase Card Program Management Office (PCPMO).

Go Back

Dashboard | Quarterly Reports

PCPMO (Level 1) Dashboard

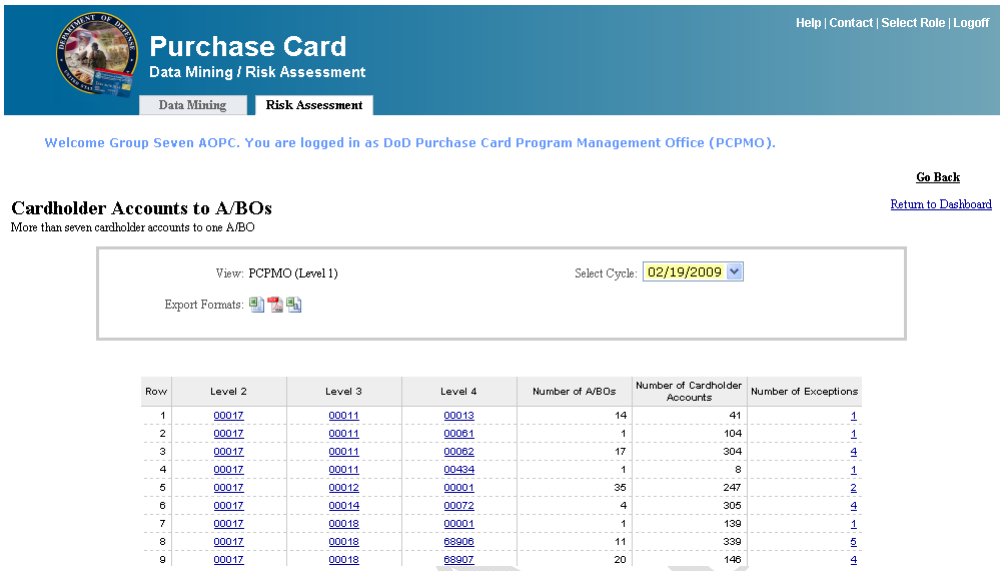
Select Cycle: 02/19/2009

Export Formats:

Control	Army				Navy				Air Force				ODA			
Overall Risk Assessment																
Category 1: Span of Control	Level 3 Risks			Control Risk	Level 3 Risks			Control Risk	Level 3 Risks			Control Risk	Level 3 Risks			Control Risk
Control 1.1: Cardholder Accounts to A/BOs More than seven cardholder accounts to one A/BO	1	8	24		17	3	0		1	1	11		5	6	13	
Control 1.2: Cardholder Accounts to A/OPCs More than 300 cardholder accounts to one A/OPC	26	5	2		20	0	0		2	3	8		17	3	4	
Category 2: Separation of Duties																
Control 2.1: Inadequate Separation of Duties Accounts for which the cardholder and A/BO are the same individual	33	0	0		20	0	0		13	0	0		24	0	0	
Category 3: Authorization Controls																
Control 3.1: Spending Ratio - Underutilized Credit Limits Accounts for which the six cycle spend average is less than 70% of the average cycle credit limit	2	8	23		3	6	11		0	1	12		5	8	11	
Control 3.2: Single Merchant Spending Accounts that have at least ten transactions and an 80% or greater spending percentage at one merchant	33	0	0		20	0	0		13	0	0		24	0	0	
Category 4: Card Status																
Control 4.1: Delinquent Accounts Managing Accounts delinquent for 30+ days	33	0	0		9	10	1		13	0	0		24	0	0	
Control 4.2: Account Usage Accounts that have been inactive for six cycles or have never been used (Excludes newly issued cards)	2	7	24		7	7	6		0	0	13		4	4	16	
Control 4.3: Lost/Stolen Cards Accounts that have greater than one lost/stolen card(s) in the last 12 cycles	33	0	0		20	0	0		13	0	0		24	0	0	
Category 5: Transaction Review Controls																
Control 5.1: Average Cycle Transactions Reviewed Higher than average number of transactions (>100) per cycle reviewed by the A/BO, based on three cycles of data	33	0	0		20	0	0		13	0	0		24	0	0	
Control 5.2: A/BO Response Rate A/BO failure to initiate case review in Case Management for flagged transactions within ten days	33	0	0		20	0	0		13	0	0		24	0	0	
Control 5.3: Flagged Transaction Determination Flagged transactions determined to be other than valid in Case Management (Misuse/Abuse/Suspected Fraud)	33	0	0		20	0	0		13	0	0		24	0	0	
Control 5.4: Convenience Check Amounts Convenience Checks over $3,000	33	0	0		20	0	0		13	0	0		24	0	0	

For Official Use Only (FOUO)

Figure 45: PCPMO Dashboard

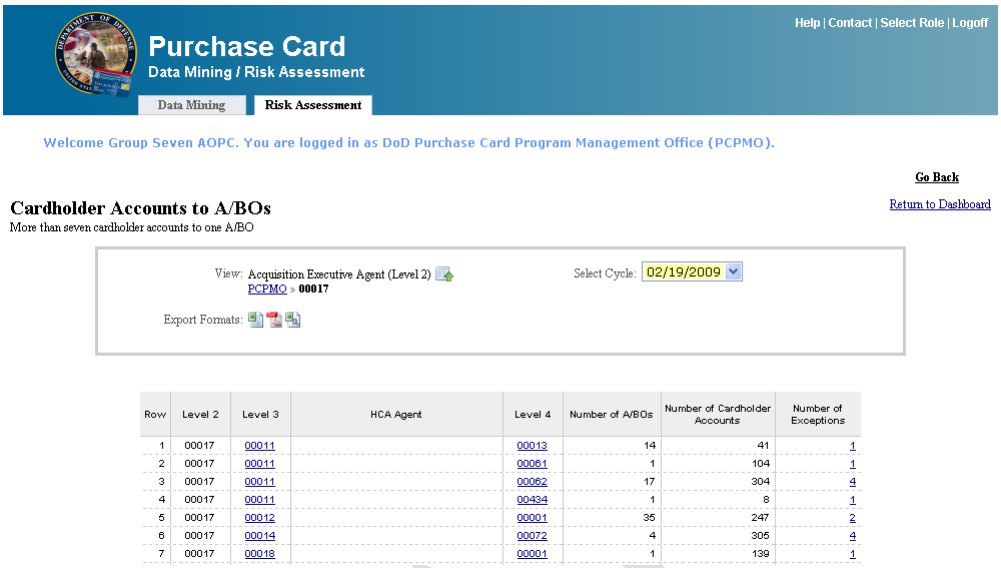


Row	Level 2	Level 3	Level 4	Number of A/BOs	Number of Cardholder Accounts	Number of Exceptions
1	00017	00011	00013	14	41	1
2	00017	00011	00061	1	104	1
3	00017	00011	00062	17	304	4
4	00017	00011	00434	1	8	1
5	00017	00012	00001	35	247	2
6	00017	00014	00072	4	305	4
7	00017	00018	00001	1	139	1
8	00017	00018	68906	11	339	5
9	00017	00018	68907	20	146	4

Figure 46: DoD PCPMO View (rows only partially listed)

Clicking on any link under Level 2, users access the Acquisition Executive Agent (Level 2) control report as shown in Figure 47 (rows only partially listed within the control report displayed in the figure).

DRAFT

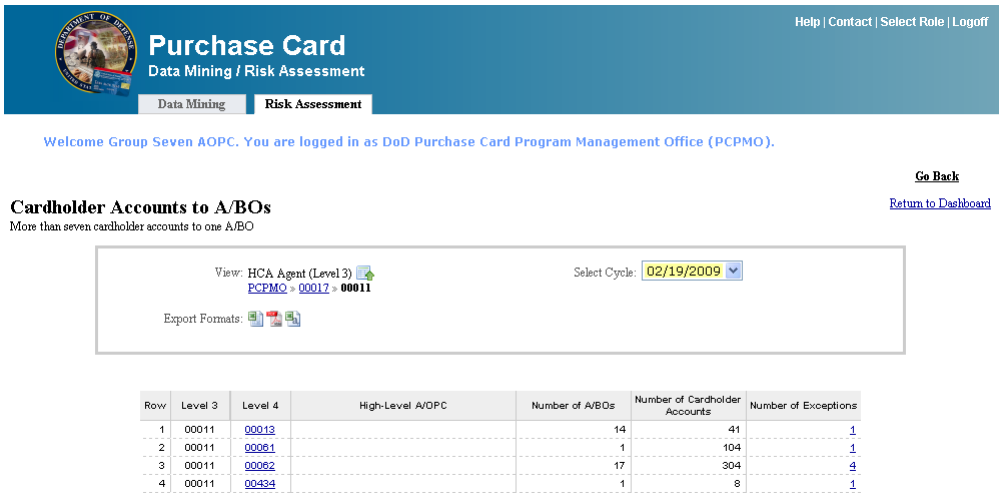


Row	Level 2	Level 3	HCA Agent	Level 4	Number of A/BOs	Number of Cardholder Accounts	Number of Exceptions
1	00017	00011		00013	14	41	1
2	00017	00011		00061	1	104	1
3	00017	00011		00062	17	304	4
4	00017	00011		00434	1	8	1
5	00017	00012		00001	35	247	2
6	00017	00014		00072	4	305	4
7	00017	00018		00001	1	139	1

Figure 47: Acquisition Executive Agent (Level 2) View (rows only partially listed)

Clicking on any link under Level 3, users access the HCA Agent (Level 3) control report as shown in Figure 48.

DRAFT



Row	Level 3	Level 4	High-Level A/OPC	Number of A/BOs	Number of Cardholder Accounts	Number of Exceptions
1	00011	00013		14	41	1
2	00011	00061		1	104	1
3	00011	00062		17	304	4
4	00011	00434		1	8	1

Figure 48: HCA Agent (Level 3) View

Clicking on any link under Level 4, users access the High-Level A/OPC control report as shown in Figure 49.

DRAFT

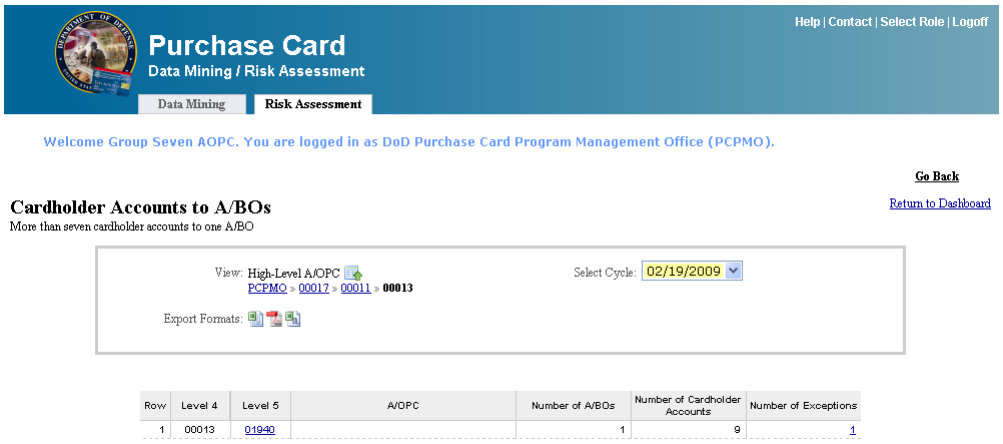


Figure 49: High-Level A/OPC View

Clicking on any link under Level 5, the Navy users access the A/OPC control report as shown in Figure 50.

DRAFT

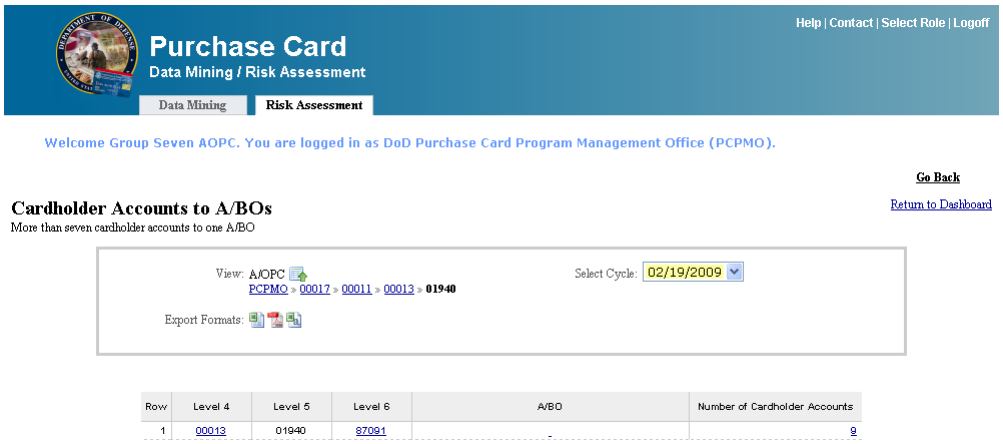
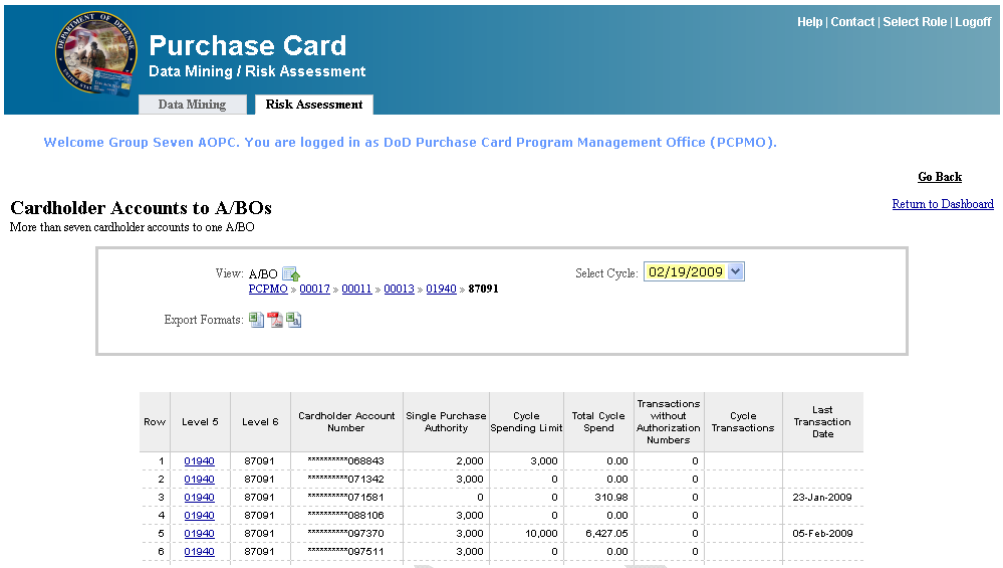


Figure 50: A/OPC View

Clicking on any link under A/BO, users access the A/BO Detail Control Report as shown in Figure 51.

DRAFT



Row	Level 5	Level 6	Cardholder Account Number	Single Purchase Authority	Cycle Spending Limit	Total Cycle Spend	Transactions without Authorization Numbers	Cycle Transactions	Last Transaction Date
1	01940	87091	**********068843	2,000	3,000	0.00	0		
2	01940	87091	**********071342	3,000	0	0.00	0		
3	01940	87091	**********071581	0	0	310.98	0		23-Jan-2009
4	01940	87091	**********088106	3,000	0	0.00	0		
5	01940	87091	**********097370	3,000	10,000	6,427.05	0		05-Feb-2009
6	01940	87091	**********097511	3,000	0	0.00	0		

Figure 51: A/BO Detail View (rows only partially listed)

DRAFT

6.7 Viewing Quarterly Reports

Quarterly Reports provide a three-billing cycle side-by-side snapshot of the exceptions under each control. This enables users to analyze progress of their purchase card program to address identified risks for the current quarter based on exception counts for the previous quarter.

Quarterly Reports are broken down into the five control categories identified in Figure 12 (page 29) and shown in Figures 52.1 through 52.5. Each category is presented as a table and displays a column for each control in the category and the exception counts for the three report billing cycles. The rows for each report are only partially listed in Figure 52.1 - 52.5.

Span of Control

Organization	Cardholders to A/BOs			Cardholders to A/OPCs		
	Apr	May	Jun	Apr	May	Jun
00060 - Doe 23, John	75	75	75	0	0	0
00041 - Doe 181, John	25	25	25	0	0	0
00042 - Doe 182, John	7	7	7	0	0	0
00043 - Doe 183, John	4	4	4	0	0	0
00044 - Doe 184, John	15	15	15	0	0	0

Figure 52.1: Quarterly Report: Span of Control Category

Separation of Duties

Organization	Inadequate Segregation of Duties		
	Apr	May	Jun
00060 - Doe 23, John	0	0	0
00041 - Doe 181, John	0	0	0
00042 - Doe 182, John	0	0	0
00043 - Doe 183, John	0	0	0
00044 - Doe 184, John	0	0	0

Figure 52.2: Quarterly Report: Separation of Duties Category

Authorization Controls

Organization	Spending Ratio - Underutilized Credit Limits			Single Merchant Spending		
	Apr	May	Jun	Apr	May	Jun
00060 - Doe 23, John	1,233	1,222	1,220	39	43	45
00041 - Doe 181, John	253	250	248	11	12	13
00042 - Doe 182, John	173	173	173	5	3	6
00043 - Doe 183, John	101	99	101	1	1	0
00044 - Doe 184, John	240	239	239	14	15	13

Figure 52.3: Quarterly Report: Authorization Controls Category

Card Status

Organization	Delinquent Accounts			Account Usage			Lost/Stolen Cards		
	Apr	May	Jun	Apr	May	Jun	Apr	May	Jun
00060 - Doe 23, John	280	269	311	1,246	1,168	1,072	0	0	0
00041 - Doe 181, John	42	49	53	333	313	293	0	0	0
00042 - Doe 182, John	35	41	34	111	95	79	0	0	0
00043 - Doe 183, John	28	27	36	100	95	93	0	0	0
00044 - Doe 184, John	50	41	52	260	244	221	0	0	0

Figure 52.4: Quarterly Report: Card Status Category

Transaction Review Controls

Organization	Average Cycle Transactions Reviewed			A/BO Response Rate			Flagged Transaction Determination			Convenience Check Amounts		
	Apr	May	Jun	Apr	May	Jun	Apr	May	Jun	Apr	May	Jun
00060 - Doe 23, John	32	33	38	2,975	3,280	3,510	1,246	1,122	1,108	91	63	90
00041 - Doe 181, John	0	1	1	502	565	562	220	190	164	17	6	7
00042 - Doe 182, John	12	12	12	590	669	747	237	253	268	25	14	37
00043 - Doe 183, John	2	1	1	156	184	211	69	68	61	6	11	2
00044 - Doe 184, John	4	3	4	632	635	679	220	187	177	13	8	7

Figure 52.5: Quarterly Report: Transaction Review Controls Category

Quarterly reports have a view specific for each Acquisition Executive Agent (Level 2), HCA Agent (Level 3), High-Level A/OPC, and A/OPC; these are not generated for A/BOs. The report shows the control exception counts for each hierarchy level directly under the user's responsibility as well as the exception counts rolled up to the user's hierarchy level.

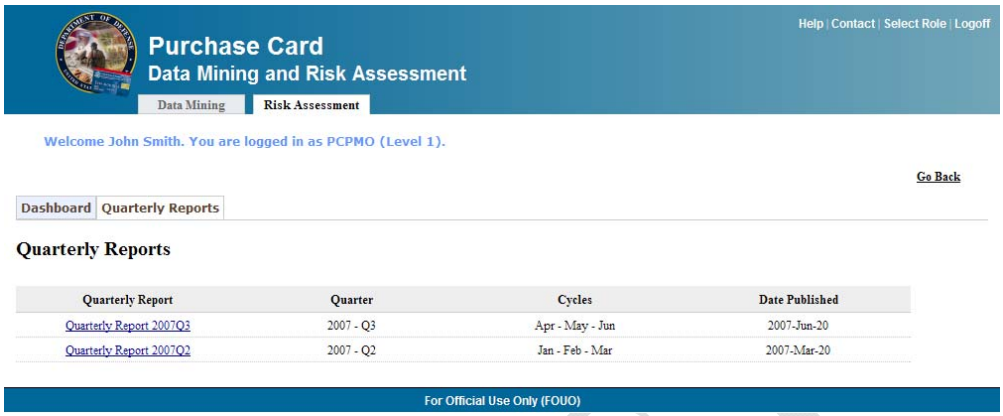


Figure 53: Quarterly Report List

Users can view their Quarterly Reports by clicking on the Quarterly Report tab that appears above the dashboard. This will take them to a list of the five most recent Quarterly Reports available to the user as shown in Figure 53. For each Quarterly Report in the list, the following information is displayed:

1. Quarterly Report title
2. Quarter of the report
3. Cycles of the quarter
4. Date the report was published.

The user accesses the report by clicking on the report title. This will open up the Quarterly Report in the PDF format.

Quarterly Report Email Notification

In addition to being able to navigate to their Quarterly Reports whenever a user is logged into the DM/RA Application, a user will also receive an email notification with a direct URL link to the Quarterly Report List page shown in Figure 53. This email will be sent to each Acquisition Executive Agent (Level 2), HCA Agent (Level 3), High-Level A/OPC, and A/OPC at the end of the quarter when the Quarterly Report is available for viewing. The A/BO does not receive the quarterly report.

DRAFT

Appendix A: Abbreviations, Acronyms, and Definitions

Abbreviations, acronyms, and terms are defined here.

AIM: Authorization, Issuance and Maintenance.

A/BO: Approving/Billing Official.

A/OPC: Agency/Organization Program Coordinator.

DM: Data Mining.

DMDC: Defense Manpower Data Center.

DoD: Department of Defense.

HCA Agent: Head Contracting Activity Agent

PCOLS: Purchase Card On-line System.

PCPMO: Purchase Card Program Management Office.

Purchase Card Abuse: Purchases of authorized goods or services at terms (e.g., price, quantity) that are excessive, for a questionable government need, or both. Examples of such transactions include purchases of items such as day planner costing $300 rather than one costing $45; allowable refreshments at excessive cost; and year-end and other bulk purchases of computer and electronic equipment for a questionable government need.

Purchase Card Fraud: Use of the government purchase card to acquire goods or services that are unauthorized and intended for personal use or gain constitute a fraud against the government. Examples include a cardholder's unauthorized purchase of power tools for his/her home; a vendor's intentional charges for services not provided; and the unauthorized use by a third party of a cardholder's compromised or stolen account for personal gain.

Purchase Card Misuse: Government purchase card transactions that are intended for government use, but are not permitted by law, regulation, or organization policy. They are generally considered improper. Examples include certain types of purchases of meals or refreshments for government employees within their normal duty stations; purchases split to circumvent micro purchase or other single purchase limits; and purchases from other than statutorily designated sources, such as the Javits-Wagner-O'Day program (JWOD).

RA: Risk Assessment.

SRS: Sign-on and Referral System.

DRAFT